Log in / create account

Navigation

- Main Page
- Community portal
- Current events
- Recent changes
- Random page
- Help

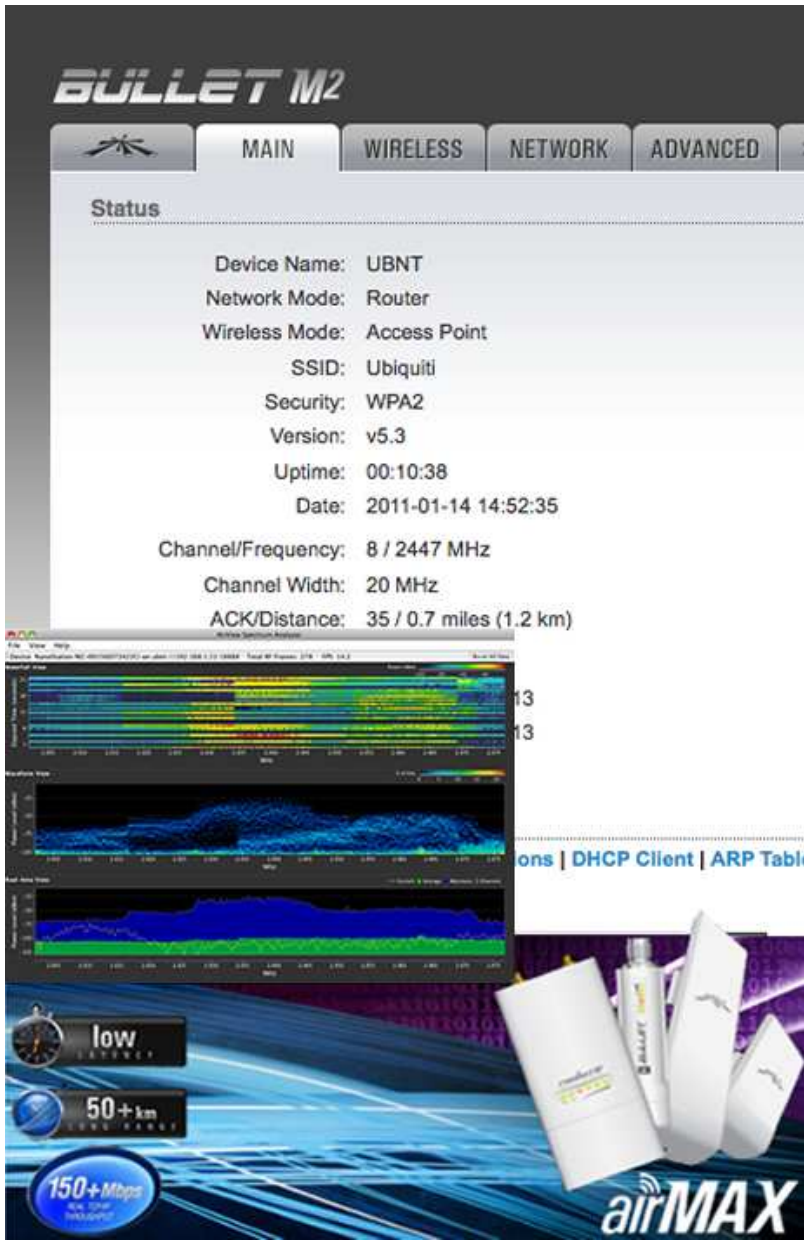
Search the Wiki

Go Search

AirOS 5.3

Contents

1 AirOS v5.3 Introduction
2 AirOS v5.3 Configuration Guide
2.1 Navigation
2.2 Ubiquiti
2.2.1 AirMax Settings
2.2.2 AirSelect
2.2.3 AirView
2.2.4 AirControl
2.3 Main Page
2.3.1 Status
2.3.2 Monitor
2.4 Wireless Page
2.4.1 Basic Wireless Settings
2.4.2 Wireless Security
2.4.2.1 WEP
2.4.2.2 WPA/WPA2
2.4.2.2.1 EAP Authentication - Station Mode
2.4.2.2.2 EAP Authentication - AP Mode
2.4.2.3 MAC ACL
2.5 Network
2.5.1 Network settings
2.5.1.1 Bridge Mode
2.5.1.2 Router Mode
2.5.1.2.1 WLAN Network Settings
2.5.1.2.2 LAN Network Settings
2.5.1.3 SOHO Router
2.5.1.3.1 WAN Network Settings
2.5.1.3.2 LAN Network Settings
2.5.1.4 VLAN Network Settings
2.5.1.5 Multicast Routing Settings
2.5.1.6 Firewall Settings
2.5.1.7 Static Routes
2.6 Advanced
2.6.1 Advanced Wireless Setting
2.6.2 Advanced Ethernet Settings
2.6.3 Signal LED Thresholds
2.6.4 Traffic Shaping
2.7 Services
2.7.1 Ping WatchDog



2.7.2 SNMP Agent
2.7.3 Web Server
2.7.4 SSH Server
2.7.5 Telnet Server
2.7.6 NTP Client
2.7.7 Dynamic DNS
2.7.8 System Log
2.8 System
2.8.1 Device
2.8.2 Date Settings
2.8.3 System Accounts
2.8.4 Miscellaneous
2.8.5 Location
2.8.6 Configuration Management
2.8.7 Device Maintenance
2.8.7.1 Firmware upload
2.9 Tools
2.9.1 Align Antenna
2.9.2 Site Survey
2.9.3 Device Discovery
2.9.4 Ping
2.9.5 Traceroute
2.9.6 Speed Test
2.9.7 AirView
2.9.7.1 Main View
2.9.7.2 Preferences

AirOS v5.3 Introduction

AirOS v5.3 is the latest evolution in Ubiquiti's AirOS interface, which includes new features like AirSelect and the latest versions of AirMax and AirView. It is an advanced operating system capable of powerful wireless and routing features, built upon a simple and intuitive user interface foundation. AirOS v5.3 maximizes the wireless performance of Ubiquiti M Series products, which are based on *IEEE 802.11n* (http://en.wikipedia.org/wiki/IEEE_802.11n) . .

AirOS v5.3 Configuration Guide

This guide presents the detailed description of the AirOS operating system version 5.3 which is integrated into all M Series products provided by Ubiquiti Networks, Inc.

M900 series (900MHz)

M2 series (2.4GHz)

M365 series (3.65GHz)

M365 series (3.65GHz)

M5 series (5GHz)

AirOS v5.3 supports the new M series product versions:

M900 (900MHz) products:

- Rocket M900 (http://ubnt.com/rocketm) ;
- Loco M900 (http://ubnt.com/nanostationm) ;

M2 (2.4GHz) products:

- Bullet M2 HP (http://ubnt.com/bulletm) ;
- Nano/Loco M2 (http://ubnt.com/nanostationm) ;
- Rocket M2 (http://ubnt.com/rocketm) ;
- PicoStation M2 HP (http://ubnt.com/picostationm)
- AirGrid M2 (http://ubnt.com/airgrid)
- NanoBridge M2 (http://ubnt.com/nanobridge)

M3 (3GHz) products:

- Rocket M3 (http://ubnt.com/rocketm) ;
- Nano M3 (http://ubnt.com/nanostationm) ;
- PowerBridge M3 (http://ubnt.com/powerbridgem)

M365 (3.65GHz) products:

- Rocket M365 (http://ubnt.com/rocketm) ;
- Nano M365 (http://ubnt.com/nanostationm) ;
- PowerBridge M365 (http://ubnt.com/powerbridgem)

M5 (5GHz) products:

- Bullet M5 HP (http://ubnt.com/bulletm) ;
- Nano/Loco M5 (http://ubnt.com/nanostationm) ;
- Rocket M5 (http://ubnt.com/rocketm) ;
- PowerBridge M5 (http://ubnt.com/powerbridgem)
- AirGrid M5 (http://ubnt.com/airgrid)
- NanoBridge M5 (http://ubnt.com/nanobridge)

All the AirOS based devices support the following infrastructure operating modes:

- Station (http://en.wikipedia.org/wiki/Station_(networking)) (Wireless Client);
- Station WDS (http://en.wikipedia.org/wiki/Wireless_Distribution_System) (Wireless Client Repeater);
- Access Point (http://en.wikipedia.org/wiki/Access_point) ;
- Access Point WDS (http://en.wikipedia.org/wiki/Wireless_Distribution_System) (Repeater).

All the AirOS v5.3 based devices support the following network modes:

- Transparent Layer2 bridge (http://en.wikipedia.org/wiki/Transparent_bridge) ;
- Router (http://en.wikipedia.org/wiki/Router) .
- SOHO Router

AirOS Quick Setup Guide describes the configuration steps for the subscriber station (wireless client - bridge) use case (AirOS v3.4 based).

All the configuration settings accessible via web management interface are described in this document (device specific elements are described individually).

Note: the examples and pictures in this document represent Nano M2, Bullet M2 and Bullet M5 graphical user interface, which is consistent between all the AirOS v5.3 based devices.

[Content]

Navigation

Each of the web management pages (listed below) contains parameters that affect a specific aspect of the device:

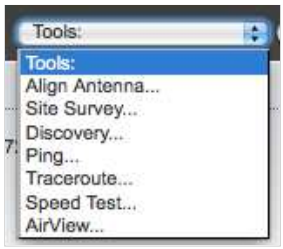
Configuration Management Menu

The **[Ubiquiti]** page contains controls for proprietary Ubiquiti technologies, such as AirMax, AirSelect and AirView.

The **[Main]** page displays current status of the device and the statistical information.

The **[Wireless]** page contains the controls for a wireless network configuration, while covering basic wireless settings which define operating mode, output power, associating details and data security options.

The **[Network]** page covers the configuration of network operating mode, IP (http://en.wikipedia.org/wiki/Internet_Protocol) settings, packet (http://en.wikipedia.org/wiki/Packet_%28information_technology%29) filtering routines and network services (i.e. DHCP Server (http://en.wikipedia.org/wiki/DHCP)).



Administration and monitoring tools

The **[Advanced]** page settings are dedicated for more precise wireless interface control. AirMax feature and 802.11n specific parameters can be set in this page. Also advanced page includes external signal LED and traffic shaping settings.

The **[Services]** page covers the configuration of system management services like SNMP (http://en.wikipedia.org/wiki/SNMP) , NTP (http://en.wikipedia.org/wiki/Network_Time_Protocol) , System Log, Ping Watchdog and SSH/Telnet server.

The **[System]** page contains controls for system maintenance routines, dedicated for administrator account management, device customization, firmware upgrade and configuration backup. Web management interface language can be changed in this page also.

There are useful network administration and monitoring **[Tools]** available in every page also:

- Antenna alignment tool;
- Site survey tool (also available in AP (http://en.wikipedia.org/wiki/Access_point) mode);
- Discovery;
- Ping (http://en.wikipedia.org/wiki/ping) ;
- Traceroute (http://en.wikipedia.org/wiki/traceroute) ;
- SpeedTest Utility;
- AirView (http://ubnt.com/airview) ;

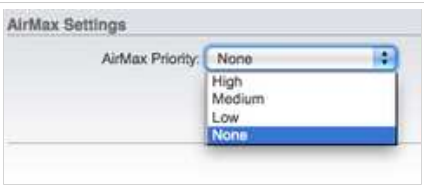
[Content]

Ubiquiti

At this page the operator can enable and setup Ubiquiti proprietary features like AirMax, allowing for superior wireless performance, more clients per Access Point and lower latency. AirSelect, an innovative technology that dynamically change the wireless channel used in order to avoid interference, as well as AirView, Ubiquiti's spectrum analyzer.

AirMax Settings

AirMax is Ubiquiti's proprietary TDMA polling technology. AirMax offers better tolerance against interference and increases the maximum number of users associated to an Access Point (AirMax capable). AirMax works assigning time slots for each device communication, avoiding the hidden node (http://en.wikipedia.org/wiki/Hidden_node_problem) problem. While operating in AP or AP-WDS mode with AirMax enabled, the device only accepts AirMax stations. (Disable AirMax for legacy 802.11abg devices compatibility). AirMax also features some advanced QOS Auto-Detection settings.



AirMax Priority (Station mode)

Enable AirMax: If enabled, the device will operate in AirMax mode, including all its benefits. But while AirMax is activated, non-AirMax stations aren't able to associate to the AP. This option only applies to AP or AP-WDS modes. In Station or Station WDS mode, AirMax will be selected automatically when connecting to an AirMax AP.

Enable AirMax and No ACK Mode for PtP (AP mode)

No ACK Mode for PtP: this option allows disabling the ACK mode for long distance (17KM in 40MHz mode or 51KM in 20MHz mode) point-to-point links exceeding the maximum ACK limit. Important: While No ACK Mode PtP is enabled, only one station can be connected. If you want to connect more than 1 station, select Auto-ACK mode.

AirMax Priority (Station mode): This feature defines the amount of timeslots assigned to each client, i.e. stations with a higher priority get more time slots to transmit over lower priority clients. AirMax Priority only functions when multiple units have it on.

AirSelect

AirSelect

AirSelect is a technology that dynamically changes the wireless channel used, in order to avoid interference and increase throughput, by hopping to the channel least used in the Frequency List (user defined) periodically within a user-defined time interval (in Milliseconds).

Enable AirSelect: if enabled, the device will use the AirSelect feature. This feature will help inexperienced installers, i.e. those without RF knowledge; or devices used in highly dynamical environments. However, it still requires good RF planning.

Frequency List: defines the channels within which AirSelect will hop to find the one less crowded.

Hop Interval: defines the time interval between each hop, expressed in milliseconds. The default value is 3000 milliseconds.

Announce Count: this is the number of times between hops the AP will announce to the clients the next hop information (frequency, etc). For instance, if hop interval is set to 10000 milliseconds, and announce count is set to 10, every 1000ms the AP will send an announcement to the clients with upcoming hop information. The larger this period is, the higher risk of timing drift (hops not being synchronized), so it is recommended to keep this hop announcement to every 100ms (or Announce Count to 1/100th of Hop Interval).

AirView

AirView

AirView is a Spectrum Analyzer included in AirOS V5.3, allowing you to see the crowdedness of the radio spectrum. A detailed step-to-step guide explaining how to use AirView is available here (http://www.ubnt.com/wiki/Best_channel_using_airview) .

AirView Port: defines the port to be used by AirView utility in this device. Default port used is 18888.

Launch AirView: press this button to launch the device's AirView Utility.

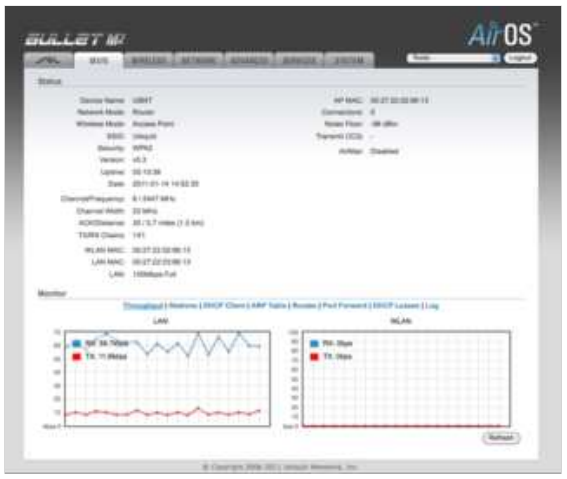
AirControl

AirControl

Enable Discovery: enables device discovery, thus the device may be discovered by other Ubiquiti devices through the Discovery Tool built-in AirOS.

Main Page

The **Main** Page displays a summary of link status information, current values of basic configuration settings (depending on operating mode), network settings and information, traffic statistics of all the interfaces.



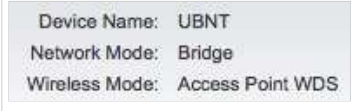
AirOS v5.3 Main Page

Status

Device Name: (http://en.wikipedia.org/wiki/Host_name) displays the customizable name (ID) of the AirOS v5.3 based device. Device Name (Host Name) will be represented in registration screens of the Router Operating Systems and discovery tools.

Network Mode: displays the device's network operating mode. AirOS v5.3 powered devices support bridge, router and SOHO router modes. The device's network mode can be changed on the Network Page.

Wireless Mode: displays the radio interface-operating mode. AirOS v5.3 powered device supports infrastructure wireless networking solution. The device's wireless mode can be changed on the Wireless Page. There are five wireless modes: Station, Station WDS, AP, AP-WDS and Spectral Analyzer (AirView). The first four could be selected on the Wireless Page. The Spectral Analyzer mode may be selected by clicking on the Tools Menu and then the AirView option. When the device is running in Spectral Analyzer mode, all wireless connections will be terminated for as long as AirView runs. Close the AirView Window to return to the previous Wireless mode.



Device Name, Wireless and Network Mode

Any M-series device may operate just in one of these modes at a time, e.g. if the device is running in AP-WDS mode it can't simultaneously run in Station mode.

AirView Status: displays the AirView Status while operating in the Spectral Analyzer mode. When AirView is running properly, the status is "Active". In case you close the AirView window the status will change to "Switching back to Station" (if the previous wireless mode was "Station"); after a few seconds, the Wireless Mode will change.

SSID (http://en.wikipedia.org/wiki/BSSID#Basic_service_set_identifier) : is the Name of the 802.11 (http://en.wikipedia.org/wiki/802.11) Service Set (established by the Access Point (http://en.wikipedia.org/wiki/Wireless_access_point) the stations are connected to):

> While operating in Station mode, displays the SSID (http://en.wikipedia.org/wiki/BSSID#Basic_service_set_identifier) of the Access Point (http://en.wikipedia.org/wiki/Wireless_access_point) where the AirOS v5.3 powered device has associated.

While operating in Access Point (http://en.wikipedia.org/wiki/Wireless_access_point) mode, displays the SSID (http://en.wikipedia.org/wiki/BSSID#Basic_service_set_identifier) of the AirOS v5.3 powered device.

Security: displays the current security setting. "None" value is displayed if wireless security is disabled. WPA or WPA2 values are displayed if the corresponding wireless security method is used. More information is provided in the *Wireless* section.

Version: shows the current firmware version. The device's firmware can be updated on the System Page. Also you can check this step-to-step tutorial (http://www.ubnt.com/wiki/index.php?title=How_To_Upgrade_Your_Firmware) for detailed instructions.

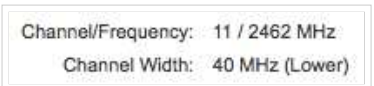
Uptime: shows the total time the device has been running since last power up (reboot) or software upgrade.

Date: indicates the current system date and time, expressed in the form "year-month-day hours:minutes:seconds". Accurate system date and time are retrieved from the Internet services using NTP (http://en.wikipedia.org/wiki/Network_Time_Protocol) (Network Time Protocol). System date and time will be set to inaccurate default values after each reboot cycle if NTP is not enabled as most of the AirOS based devices have no autonomous power supply for the internal clock.

Total uptime and device date

Channel/Frequency: (http://en.wikipedia.org/wiki/Frequency) This is the operating frequency of the 802.11 (http://en.wikipedia.org/wiki/802.11) Service Set (hosted by AP) the client is connected to. 802.11 (http://en.wikipedia.org/wiki/802.11) Channel (http://en.wikipedia.org/wiki/Channel_%28communications%29) number corresponds to the operating frequency (http://en.wikipedia.org/wiki/Frequency) . More information about the supported channels is provided in the *Wireless* section. Device uses the radio frequency (http://en.wikipedia.org/wiki/Frequency) specified to transmit and receive data. For 5 GHz operation (M5 series), the common range of available frequencies (channels) is 5.1-5.9GHz, for 2.4 GHz operation (M2 series) - 2412-2472MHz, for 900MHz operation (M900 series) - 902-928MHz, for 3GHz operation (M3 series) - 3300-3700MHz, and for 3.65GHz operation (M365 series) - 3650-3675MHz. Valid frequency range (channels) will vary depending on local country regulations. For more information regarding frequency support, please visit the compliance section (http://www.ubnt.com/wiki/RF_Compliance) of the Ubiquiti Wiki.

Channel Width: This is spectral width of the radio channel used by AirOS v5.3 powered device. 5, 10, 20 and 40 MHz channel spectrum widths are supported. In Station (or Station WDS) Auto 20/40MHz is the value by default.



Current channel and channel width

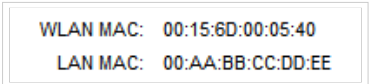
ACK Timeout (http://en.wikipedia.org/wiki/802.11#Frames) : displays the current timeout value for ACK frames. ACK Timeout can be set manually or self-adjusted automatically. The **ACK Timeout** (http://en.wikipedia.org/wiki/802.11#Frames) (Acknowledgement frame Timeout) specifies how long the AirOS device should wait for an acknowledgement from a partner device confirming packet reception before concluding the packet must have been in error and requires resending. ACK Timeout is a very important outdoor wireless performance parameter. When you are using 802.11n mode, it is recommended to set "Auto adjust" for ACK Timeout. More information is provided in the *Advanced* settings section.

TX/RX Chains: displays the number of independent spatial data streams AirOS v5.3 powered device is transmitting/receiving simultaneously within one spectral channel of bandwidth. This ability is specific for 802.11n (http://en.wikipedia.org/wiki/IEEE_802.11n) devices that rely on multiple-input multiple-output (MIMO) (http://en.wikipedia.org/wiki/Multiple-input_multiple-output) technology. Multiple chains increase data transfer performance significantly. **The number of chains Ubiquiti device uses are hardware specific**. Every TX/RX chain requires separate antenna. Bullet M series devices use 1 chain for transmitting/receiving (1x1). Nano/Loco M series and Rocket M series uses 2 chains for transmitting/receiving (2x2).

ACK Timeout/Distance and TX/RX Chains

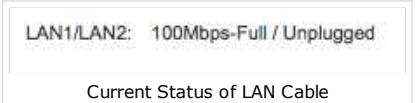
WLAN MAC: displays the MAC address (http://en.wikipedia.org/wiki/MAC_Address) of the AirOS v5.3 device WLAN (http://en.wikipedia.org/wiki/Wireless_LAN) (Wireless) interface.

LAN MAC: displays the MAC address (http://en.wikipedia.org/wiki/MAC_Address) of the AirOS v5.3 device LAN (http://en.wikipedia.org/wiki/Lan) (Ethernet (http://en.wikipedia.org/wiki/Ethernet)) interface.



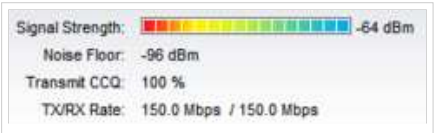
LAN and WLAN MAC

LAN1/LAN2: indicates the current status of the Ethernet (http://en.wikipedia.org/wiki/Ethernet) port(s) connection. This can alert the system operator-technician that LAN (http://en.wikipedia.org/wiki/LAN) cable is not plugged into the device and there is no active Ethernet (http://en.wikipedia.org/wiki/Ethernet) connection. When cable is plugged in, negotiated data rate will be displayed; possible rates are 10Mbps or 100Mbps, or else Half duplex or Full duplex.



Current Status of LAN Cable

AP MAC: displays the MAC address (http://en.wikipedia.org/wiki/MAC_Address) of the Access Point (http://en.wikipedia.org/wiki/Wireless_access_point) where the device has associated while operating in Station mode (or Station WDS). It is the MAC address of the AirOS v5.3 powered device's wireless interface itself if operating in Access Point mode. AP MAC is used as Basic Service Set Identifier (BSSID) (http://en.wikipedia.org/wiki/BSSID) in infrastructure type wireless networks.



Status information available in AirOS powered Station

MAC (http://en.wikipedia.org/wiki/Media_Access_Control) is unique HW (http://en.wikipedia.org/wiki/Hardware) identifier on each 802.11 (http://en.wikipedia.org/wiki/802.11) radio. It consists of two parts:

An Organizationally Unique Identifier (OUI (http://en.wikipedia.org/wiki/Organizationally_Unique_Identifier))
Network Interface Controller (NIC (http://en.wikipedia.org/wiki/Network_Interface_Controller)) sequence.

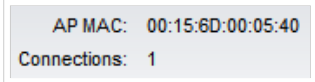
The manufacturer list of a given MAC address (http://en.wikipedia.org/wiki/MAC_Address) is provided in this (http://standards.ieee.org

/regauth/oui/index.shtml) page.

Signal Strength: (http://en.wikipedia.org/wiki/Signal_strength) displays the received wireless (http://en.wikipedia.org/wiki/Wireless) signal level (client-side) while operating in Station mode. The represented value coincides with the graphical bar. Use antenna alignment tool to adjust the device antenna to get better link with the wireless device. The antenna of the wireless client has to be adjusted to get the maximum signal strength. Signal Strength (http://en.wikipedia.org/wiki/Signal_strength) is measured in dBm (the Decibels referenced to 1 miliwatt). The conversion is defined as dBm=10log10(P/1mW). So, 0dBm would be 1mW and −72dBm would be .0000006mW. A signal strength of −80dBm or better (-50..-70) is recommended for stable links.

Connections: displays the number of associated wireless stations while the device is operating in Access Point mode. This value is not displayed while operating in Station mode.

Horizontal/Vertical: displays the wireless signal levels received for each polarity, while operating in Station (or Station WDS) mode on MIMO 2x2 devices. Signals Strength are measured in dBm.

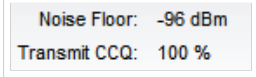


AP MAC address and Connections (wireless stations associated)

Noise Floor: displays the current value of the noise (http://en.wikipedia.org/wiki/Electronic_noise) level in dBm. Noise Floor (http://en.wikipedia.org/wiki/Noise_floor) is taken into account while evaluating the signal quality (Signal-to-Noise Ratio SNR, RSSI) while value mean depends on signal strength above the noise floor.

Transmit CCQ: This is an index of which evaluates the wireless Client Connection Quality. The level is based on a percentage value where 100% corresponds to a perfect link state.

TX Rate and RX Rate: displays the current 802.11 (http://en.wikipedia.org/wiki/802.11) data transmission (TX) and data reception (RX) rate while operating in *Station* mode. Data rates up to 150 Mbps on 1 chain devices (Bullet M series) and up to 300 Mbps on 2 chain devices (NanoStation/LocoStation M and Rocket M series) can be used. Highest data rates will provide maximum data throughput while signal level is relevant.

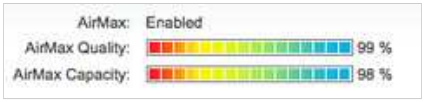


Noise Floor and Transmit CCQ

Airmax: Indicates the current status of the AirMax (Ubiquiti's proprietary TDMA polling technology) in the device while operating in AP or AP WDS mode. If AirMax is enabled, the device only accepts AirMax stations. (Disable AirMax for legacy 802.11abg devices compatibility). AirMax also features some advanced QOS AutoDetection settings.

Airmax Quality: This is an index that evaluates the AirMax Connection Quality. The level is based on a percentage value where 100% corresponds to a perfect link state.

Airmax Capacity: This is an index of maximum data rate the link is operating at. A Lower Capacity number indicates a unit that is bogging the system down.

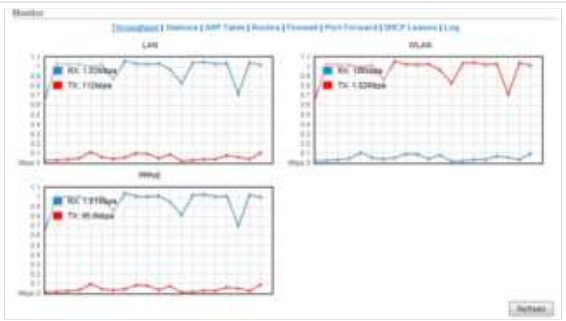


Airmax status, Airmax quality and capacity

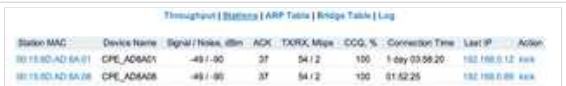
[Content]

Monitor

Throughput: shows graphs that continuously represent the current data traffic on the LAN, WLAN and PPP interfaces in both graphical and numerical format. The chart scale and throughput dimension (Bps, Kbps, Mbps) changes dynamically according to the mean throughput value. The statistics are updated automatically. Throughput statistics can be updated manually using the *Refresh* button.


Throughput graphs and statistics

Stations: this selection lists the stations which are connected to the device while operating in Access Point mode (or Access Point WDS).


Status Reporting in AP mode

The following statistics for every station associated is represented in the station statistics window:

Station MAC of the station which is associated;

Device Name: displays the client's host name associated to the respective AP. The *device name* could be change on the System Page.

Signal/Noise, dBm Signal value represents the last received wireless signal level, and Noise displays the value of the noise level wireless signal was received;

ACK: these values indicate the ACK Timeout and its corresponding distance to the station.

Tx/Rx, Mbps Tx value represents the data rates, in Mbps, of the last transmitted packets, and Rx value represents the data rates, in Mbps, of the last received packets;

CCQ, %: This is an index of which evaluates the wireless Client Connection Quality. The level is based on a percentage value where 100% corresponds to a perfect link state.

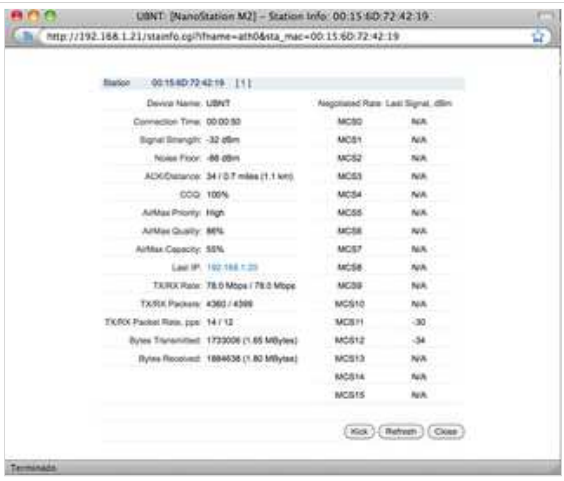
Connection time: this value represents the total time running of the stations associated to the AP. The time is expressed in days, hours, minutes and seconds.

Last IP: displays the last station's IP address associated to the AP.

Action: shows available options for this station, e.g.: kicking a station for a few seconds to identify any problematic stations.

The information in the station statistics window can be updated using the *Refresh* button.

Detailed information can be retrieved while selecting the particular *MAC* of the associated station:

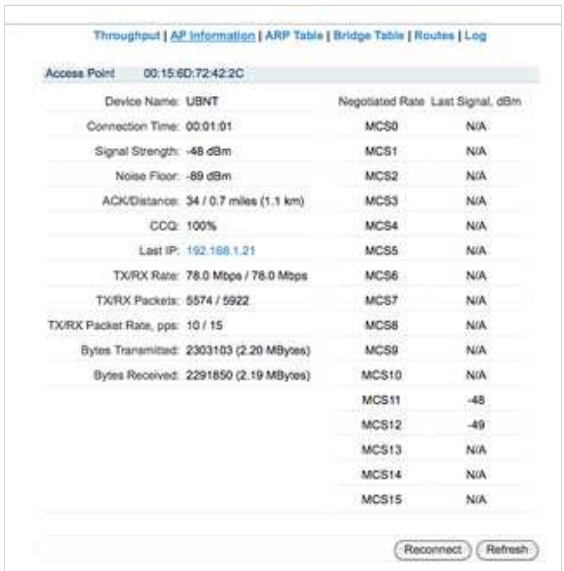


Station info

Device Name :displays the client's host name associated to the respective AP. The device name could be change on the System Page.
Connection time value represents the running total of time the station is associated. The time is expressed in days, hours, minutes and seconds;
Signal Strength value represents, in dBm, the last received wireless signal level;
Noise Floor: displays the current value of the noise (http://en.wikipedia.org/wiki/Electronic_noise) level in dBm. Noise Floor (http://en.wikipedia.org/wiki/Noise_floor) is taken into account while evaluating the signal quality (Signal-to-Noise Ratio SNR, RSSI) while value mean depends on signal strength above the noise floor.
ACK/Distance: these values indicate the ACK Timeout and its corresponding distance to the station.
CCQ value represents the quality of the connection to the Station;
Last IP: displays the last station's IP address associated to the AP.
Tx/Rx Rate represents the data rates, in Mbps, of the last transmitted and received packets;
Tx/Rx Packets value represents the total amount of packets transmitted to and received from the Station during the connection uptime;
Tx/Rx Packet Rate, pps represents the mean value of the transmitted and received packet rate;
Bytes transmitted value represents the total amount of data (in bytes) transmitted during the connection;
Bytes received value represents the total amount of data (in bytes) received during the connection;
Negotiated Rate/Last Signal (dBm) table values represent the received wireless signal level along with the all data rates of recently received packets. "N/A" value is represented as the *Last Signal* if no packets were received on that particular data rate.

The information in the statistic window is updated automatically. The information in the station statistics window can be updated using the *Refresh* button. Window can be closed with the **Close this window** button.

AP Information: selection opens the connection statistics window while operating in Station mode.



Status Reporting in Station mode

The following link statistics is provided:
Access Point shows MAC address of the Access Point station is associated to;
Device Name: displays the host name of the Access Point the station is associated to.
Connection time value represents the running total of time the station is associated to the AP. The time is expressed in days, hours, minutes and seconds;
Signal Strength value represents the last received wireless signal level;
Noise Floor: displays the current value of the noise (http://en.wikipedia.org/wiki/Electronic_noise) level in dBm. Noise Floor (http://en.wikipedia.org/wiki/Noise_floor) is taken into account while evaluating the signal quality (Signal-to-Noise Ratio SNR, RSSI) while value mean depends on signal strength above the noise floor.
ACK/Distance: these values indicate the ACK Timeout and its corresponding distance to the AP.
CCQ value represents the quality of the connection to the AP;
Tx/Rx Rate represents the data rates of the last transmitted and received packets;
Tx/Rx Packets value represents the total amount of packets transmitted and received during the connection;
Tx/Rx Packet Rate (packets per second) represents the mean value of the transmitted and received packet rate;
Bytes transmitted/received value represents the total amount of data (in bytes) transmitted and received during the connection;
Negotiated Rate/Last Signal (dBm) table values represent the received wireless signal level along with the all data rates of recently received packets. "N/A" value is represented as the *Last Signal* if no packets were received on that particular data rate.

To reconnect to the AP press the **Reconnect** button, in order to reestablish the wireless link

The list can be updated using the **Refresh** button.

DHCP Client: (Applicable for Router - DHCP mode only) shows the device's WAN IP address, Netmask, DNS servers and Gateway while operating in DHCP Router mode.

DHCP Client in Station mode

IP Address: displays the device's WAN IP address while operating in DHCP - Station mode.
Netmask:displays the device's netmask when operating in DHCP Client mode. It is assigned automatically by the DHCP server (not the device's DHCP server), which assigns the WAN IP address to the device.

Gateway: displays the device's gateway when operating in DHCP Client mode, which is assigned automatically by the DHCP server (not the device's DHCP server).
Primary/Secondary DNS IP: Domain Name System (DNS) is an Internet "phone book" which translates domain names to IP addresses. These fields identify the server IP addresses of where the AirOS device looks for the translation source.
DHCP Server: displays the IP address of the DHCP Server assigning the device's WAN IP Address.
Total Lease Time: shows the total time (validity) of the leased IP address assigned by the external DHCP server.
Remaining Lease Time: displays the remaining time of the IP address leased by the external DHCP server.

ARP Table: selection lists all the entries of the ARP (Address Resolution Protocol) table currently recorded on the device.

Throughput | Stations | ARP Table | Bridge Table | Routes | Log
IP Address MAC Address Interface
192.168.0.49 00:0C:76:F5:86:27 BRIDGE
192.168.0.69 00:25:00:41:26:65 BRIDGE
192.168.0.1 00:09:A3:00:4B:8E BRIDGE
192.168.0.67 00:18:39:98:D4:8A BRIDGE
192.168.0.6 00:0D:87:BB:86:E5 BRIDGE
Refresh
ARP table

The list can be updated using the **Refresh** button.

ARP is used to associate each IP address to the unique hardware address (MAC) the devices. It is important to have unique IP addresses for each MAC or else there will be ambiguous routes in the network.

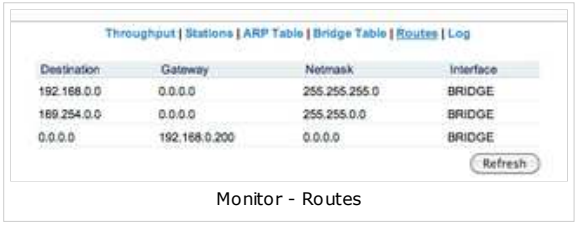
Bridge Table: selection lists all the entries in the system bridge table, while the device is operating in *Bridge* mode.

The list can be updated using the **Refresh** button.

Bridge table shows to which *bridge* port the particular station is associated to - in other words, from which *interface* (Ethernet or wireless) the network device (defined by *MAC address*) is reachable to AirOS system while forwarding the packets to that port only (thus saving a lot of redundant copies and transmits).

Ageing timer shows ageing time for each address entry (in seconds) - after particular time out, not having seen a packet coming from a certain address, the bridge will delete that address from the Bridge Table.

Routes: selection lists all the entries in the system routing table, while the device is operating in *Router* mode.


Throughput | Stations | ARP Table | Bridge Table | Routes | Log
Destination Gateway Netmask Interface
192.168.0.0 0.0.0.0 255.255.255.0 BRIDGE
169.254.0.0 0.0.0.0 255.255.0.0 BRIDGE
0.0.0.0 192.168.0.200 0.0.0.0 BRIDGE
Refresh
Monitor - Routes

The list can be updated using the **Refresh** button.
AirOS examines the *destination IP address* of each data packet traveling through the system and chooses the appropriate interface to forward the packet to. The system choice depends on static routing rules – entries, which are registered in the system routing table. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of all the AirOS interfaces.

AirOS IP configuration description is provided in the *Wireless* section.

Firewall: selection lists active firewall entries in the *FIREWALL chain* of the standard ebtables (http://ebtables.sourceforge.net/ebtables-man.html) *filter table*, while the device is operating in *Bridge* mode.

Monitor - Firewall

The list can be updated using the '*Refresh* button.
Active firewall entries in the *FIREWALL chain* of the standard iptables (http://security.maruhn.com/iptables-manual.html) *filter table* are listed if the device is operating in *Router* mode.

The list can be updated using the **Refresh** button.

IP and MAC level access control and packet filtering in AirOS is implemented using iptables (http://security.maruhn.com/iptables-manual.html) (routing) and ebtables (http://ebtables.sourceforge.net/ebtables-man.html) (bridging) firewall that protects the resources of a private network from outside threats by preventing unauthorized access and filtering specified types of network communication.

More information is provided in the *Wireless* section.

Port Forward: selection lists active port forward entries in the *PORTFORWARD chain* of the standard iptables (http://security.maruhn.com/iptables-manual.html) *nat table*, while the device is operating in *Router* mode.

Monitor - Port forwarding

The list can be updated using the **Refresh** button.

Port Forwarding creates a transparent tunnel through a firewall/NAT, granting an access from the WAN side to the particular network service running on the LAN side.

DHCP Leases: selection shows the current status of the leased IP addresses by the device's DHCP server. This option is available if *DHCP Server* is enabled while the device is operating in *Router* mode.

Throughput | AP Information | DHCP Client | ARP Table | Routes | Port Forward | DHCP Leases | Log
MAC Address IP Address Remaining Lease Hostname Interface
00:25:4B:A9:7B:5A 192.168.4.143 00:55:32 LAN
Refresh
DHCP leases

MAC address shows the client's MAC address, which is connected to the Access Point.
IP address shows the client's IP address leased by the device's DHCP server.
Remaining Lease time shows for how long the leased *IP address* will be valid and reserved for particular DHCP client.
Hostname: displays the device name (hostname) of the client receiving an IP lease.
Interface name shows from which device the interface DHCP client specifying *MAC Address* is connected.

The list can be updated using the **Refresh** button.

More information is provided in the *Wireless* section.

Log selection shows a list with all the registered system events.

All the entries in the system log will be deleted if the **Clear** button is activated. The *System Log* content is updated if **Refresh** button is activated.

Message "Syslog is disabled, unable to show system messages" is displayed if the *System Log* is not enabled. *System Log* configuration description is provided in the *Services* section.

[Content]

Wireless Page

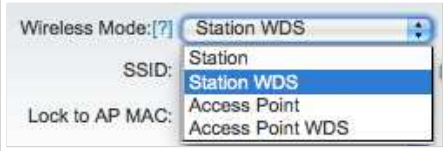
The Wireless Page contains everything needed by the operator to setup the wireless part of the link. This includes regulatory requirements, SSID, channel and frequency settings, device mode, data rates, and wireless security.

Wireless Page – NanoStation M2

Basic Wireless Settings

The general wireless settings, such as the wireless device BSSID, country code, output power, 802.11 mode and data rates can be configured in this section.

Wireless Mode: specifies the operating mode of the device. The mode depends on the network topology requirements. There are 4 operating modes supported in AirOS v5.3 software:



Wireless Mode

1. **Station**: This is a client mode, which can connect to an AP.
It is common for a bridging application to an AP. In *Station* mode device acts as the Subscriber Station while connecting to the Access Point, which is primary defined by the SSID and forwarding all the traffic to/from the network devices connected to the Ethernet interface.
The specifics of this mode is that Subscriber Station is using *arpnat* technique which may result lack of transparency while passing-through *broadcast* packets in *bridge* mode.

2. **Station WDS**: WDS stands for Wireless Distribution System. Station WDS should be used while connecting to the Access Point, which is operating in WDS mode. This mode is compatible with WPA/WPA2 encryption.
Station WDS mode enables packet forwarding at layer 2 level.
The benefit of *Station WDS* is improved performance and faster throughput. *Station WDS - Bridge* mode is fully transparent for all the Layer2 protocols.
Refer to the section Network Settings for detailed Bridge network mode configuration information.

3. **Access Point**: This is an 802.11 Access Point (http://en.wikipedia.org/wiki/Access_point)

4. **Access Point WDS**: This is an 802.11 Access Point (http://en.wikipedia.org/wiki/Access_point) which allows for layer 2 bridging with Station WDS devices using the WDS protocol. AP WDS is not fully compatible with WPA/WPA2 encryption.
WDS allows you to bridge wireless traffic between devices that are operating in *Access Point* mode. Access Point is usually connected to a wired network (Ethernet LAN) allowing wireless connection to the wired network. By connecting Access Points to one another in an Extended Service Set using the WDS, distant Ethernets can be bridged into a single LAN.

It is very important that network loops should not be created with either WDS bridges or combinations of wired (Ethernet) connections and WDS bridges. Tree or Star shape network topology should be used in all WDS use-cases (i.e. if AP2 and AP3 are specified as the WDS peers of AP1, AP2 should not be specified as the WDS peer of AP3 and AP3 should not be specified as the WDS peer of AP2 in any case). Mesh and Ring network topologies are not supported by WDS and should be avoided in all the use cases.

Note: *Station WDS* and *AP WDS* mode uses the WDS protocol that is not defined as the standard thus compatibility issues between equipment from different vendors may arise.

Note: When connecting devices in AP-WDS-to-AP-WDS mode, the WPA/WPA2 security methods will not function. When connecting AP-WDS devices to another AP-WDS device use none or the WEP security method. However, this may compromise the security of your network. In case of connecting STA-WDS clients to an AP-WDS device, all security methods are available and work properly.

WDS Peers: WDS Stations and/or WDS Access Points connected to the AirOS powered Access Point should be specified in this list in order to create a wireless network infrastructure - Wireless Distribution System (applicable to AP WDS mode only).

WDS Peers

Enter the MAC address of the paired WDS device in the WDS Peer entry field. One MAC address should be specified for a Point-to-Point connection use case, up to six WDS Peers can be specified for a Point-to-Multi-Point connection use case.

Auto option should be enabled in order to establish WDS connection between Access Points if *WDS Peers* are not specified (applicable to AP WDS mode only). If *Auto* option is enabled AirOS powered Access Point will choose WDS Peers

(Access Points) according to the SSID setting. Access Point operating in WDS mode should have the same SSID as the WDS Peer in order to establish the connection automatically while **Auto** option is enabled. This configuration is also known as the *repeater* mode. AP WDS **Auto** option cannot be selected if any type of WPA or WPA2 security is used as WPA requires different roles on AP configuration (authenticator or supplicant).

Note: Access Point operating in WDS mode and all the WDS Peers must operate on the same frequency *channel*, use the same *channel spectrum width* and the same security settings.

SSID and hide SSID (AP Mode)

SSID: Service Set Identifier used to identify your 802.11 wireless LAN should be specified while operating in *Access Point* or *Access Point WDS* mode. All the client devices within the range will receive broadcast messages from the access point advertising this SSID.

While operating in Station or Station WDS mode, you should specify the SSID of the Access Point the AirOS v5.3 device is associated to. There can be several Access Points with an identical SSID. If the SSID is set to "Any" the station will connect to any available AP.

SSID and Site Survey (Select) tool (Station Mode)

The list of the available Access Points can be retrieved using the **Select** button (not applicable to Access Point mode). This control activates *Site Survey* tool that is used for the AP selection. Site Survey will search for the available wireless networks in the range on all the supported channels and will allow you to select one for association. In case the selected network uses encryption, you'll need to set security parameters in *Wireless Security* section. Select the Access Point from the list and click **Select** button for association.

Click **Scan** button to refresh the list of available wireless networks. Site Survey channel scan list can be modified using the *Channel Scan List* control.

Look to AP MAC option

Hide SSID control will disable advertising the SSID of the access point in broadcast messages to wireless stations. Unselected control will make SSID visible during network scans on the wireless stations. Control is available while operating in *Access Point* mode only.

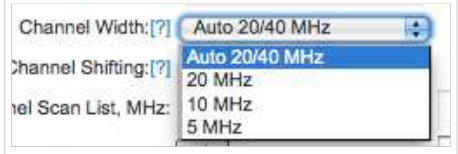
Lock to AP MAC: This allows the station to always maintain connection to a particular AP with a specific MAC (applicable to Station and Station WDS mode only). This is useful as sometimes there can be few identically named SSID's (AP's) with different MAC addresses. With AP lock on, the station will lock to MAC address and not roam between several Access Points with the same ESSID.

Country Code: Different countries will have different power levels and possible frequency selections. To ensure device operation follows regulatory compliance rules, **please make sure to select your correct country where the device will be used**. The channel list, output power limits, IEEE 802.11 and Channel Spectrum Width modes will be tuned according to the regulations of the selected country. Additionally, please consult the compliance guide (http://www.ubnt.com/wiki/RF_Compliance) for further explanation of international compliance requirements.

IEEE 802.11 mode and Country Code selection - NanoStation M2

IEEE 802.11 Mode: This is the radio standard used for operation of your AirOS powered device. 802.11b, 802.11a and 802.11g are old 2.4GHz mode, while the 802.11n (2.4GHz and/or 5GHz) is newer standards based on faster Orthogonal Frequency Division Multiplexing (OFDM) modulation. For more information, please consult 802.11 compliance guide (http://www.ubnt.com/wiki/RF_Compliance) .

- M900 Series devices supported IEEE 802.11 mode:
  A/N mixed – connect to an 802.11a or 802.11n network (selected by default). This mode offers better compatibility.
- M2 Series devices supported IEEE 802.11 mode:
  B/G/N mixed – connect to an 802.11b, 802.11g or 802.11n network (selected by default). This mode offers better compatibility.
- M3 Series devices supported IEEE 802.11 mode:
  A/N mixed – connect to an 802.11a or 802.11n network (selected by default). This mode offers better compatibility.
- M365 Series devices supported IEEE 802.11 mode:
  A/N mixed – connect to an 802.11a or 802.11n network (selected by default). This mode offers better compatibility.
- M5 Series devices supported IEEE 802.11 mode:
  A/N mixed – connect to an 802.11a or 802.11n network (selected by default). This mode offers better compatibility.



Select the Channel Spectrum Width

Channel Width: This is the spectral width of the radio channel. Supported wireless channel spectrum widths:

5MHz – is the channel spectrum with the width of 5 MHz (known as Quarter-Rate mode).
10MHz – is the channel spectrum with the width of 10 MHz (known as Half-Rate mode).
20MHz – is the standard channel spectrum width (selected by default).
40MHz – is the channel spectrum with the width of 40 MHz.
Auto 20MHz/40MHz – only available in Station (or Station WDS) mode. It offers better compatibility.

Reducing the spectral width provides 2 benefits and 1 drawback.

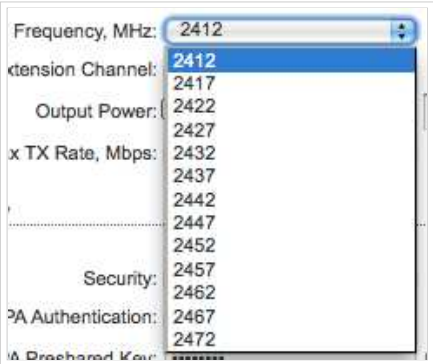
Benefit 1: It will increase the amount of non-overlapping channels. This can allow networks to scale better.
Benefit 2: It will increase the PSD (power spectral Density) of the channel and enable the link distance to be increased.

Drawback: It will reduce throughput proportional to the channel size reduction. So just as turbo mode (40MHz) increases possible speeds by 2x, half spectrum channel (10MHz), will decrease possible speeds by 2x.

Enable or disable Channel Shifting

Channel Shifting: enables special channels with a frequency offset regarding standard 802.11b/g/n and 802.11a channels. This is a proprietary Ubiquiti developed feature. While 802.11 networks have standard channels, e.g. Channel 36 (5180MHz), Channel 40 (5200MHz), etc. with intervals of 5MHz; channel shifting will allow operation of new non-802.11 channels offset from the standard channels. All the channels can be shifted from the default central channel frequency in intervals of 5 MHz (in 802.11na) or 2/3 MHz (in 802.11bgn).

The benefits of these options are private networking and inherent security. Using channel-shifting, networks can instantly become invisible to the millions of Wi-Fi devices in the world.

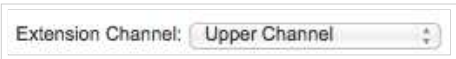


Select a Wireless Frequency on NanoStation M2

Frequency, MHz: select the wireless channel while operating in *Access Point* mode. Multiple frequency channels are available to avoid interference between nearby access points. The channel list varies depending on the selected country code, IEEE 802.11 mode and Channel Spectrum Width and Channel Shifting option. Now AirOS 5.3 incorporates the "Auto" option that selects the best channel, based on current utilization and noise, when the devices is initialized or restarted. Once the channel is selected, it will remain on that channel until the radio is rebooted, or additional changes are made.

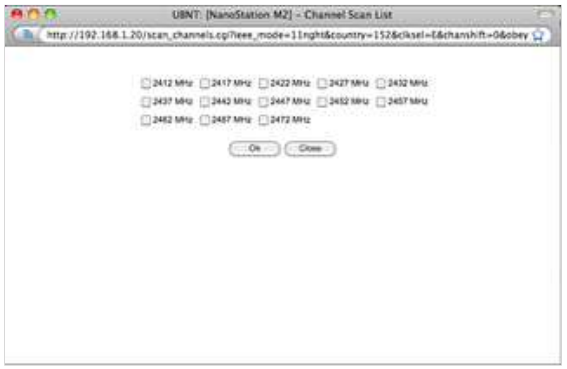
Extension Channel: (Only applicable to AP or AP WDS, and 40MHz channel width) indicates the use of channel bonding that allows the AirMax network to use two channels at once. Using two channels improves the performance of the Wi-Fi connection. It is automatically selected by the system.

Channel Scan List, MHz: This will confine scanning only to the selected channels (applicable to Station and Station WDS mode only). The benefits of this are faster scanning as well as filtering out unwanted AP's in the results. Site Survey tool will look for the Access Points in selected channels only.



Extension Channel

Frequency List, MHz: when this option is enabled, it can be used for two proposes: firstly with the "Auto" frequency selected, the listed frequencies will be scanned and analyzed (values can be typed in manually, separated by commas, or picking channels through the "Edit" option). Secondly with the feature enabled and AirSelect running, AirSelect will use only channels specified in the Frequency List.



Channel Scan list selection on NanoStation M2,country:Chile

Channel list management for the selected IEEE 802.11 mode and specified Channel Spectrum Width can be enabled by selecting the **Enabled** option. There are two ways to set the Channel Scan List - enumerating the required channels (separated by comma) in the input field or using the selection options in Channel Scan List window, which is activated using the **Edit** button. *Site Survey* tool will look for the Access Points in selected channels only if the scan or site survey operation is performed in *Station* mode.

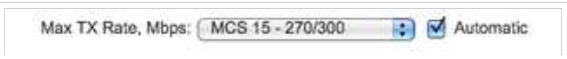
Antenna Gain:specifies the gain of the antenna installed in the AP (applies only to devices with external antenna connector, such as Rocket and Bullet). When "Obey Regulatory Rules" is enabled, the antenna gain calculates the TX power backoff needed to remain in compliance with local regulations. This feature is complementary to the "Cable Loss" feature; and both affect the TX power of the unit.

Cable Loss: When "Obey Regulatory Rules" is enabled, the Cable Loss affects the TX power of the unit. In case you have high amounts of cables loss, the higher TX power may be increased while being in compliance with the maximum TX power allowed by the local authority. This feature is complementary to the "Antenna Gain" feature.

Output power and Obey regulatory power

Output Power: This will configure the maximum average transmit output power (in dBm) of the wireless device. The output power at which wireless module transmits data can be specified using the slider. When entering output power value manually, the slider position will change according to the entered value. The transmit power level maximum is limited according to the country regulations. If the AirOS v5.3 based device has an internal antenna (i.e. NanoStation M/LocoStation M), Output Power is the output power delivered to the internal antenna.

Obey regulatory Rules option must remain enabled while it will force the transmit output power to be compliant with the regulations of the selected country. In this case, it will not be possible to set equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain (different maximum output power levels and antenna gains are allowed for each IEEE 802.11a/b/g/n regulatory domain thus country). For more regulatory information, please consult 802.11 compliance guide (http://www.ubnt.com /wiki/RF_Compliance) .



Wireless Data rate

Max Data Rate, Mbps: This defines the data rate (in Mbps) at which the device should transmit wireless packets. You can fix a specific data rate between MCS 0 and MCS 7 (or MCS15 for 2x2 chains devices) also. It is recommended to use automatic option, especially if you are having trouble getting connected or losing data at a higher rate. In this case, the device will use the lower data rates automatically.. If you select 20MHz Channel Spectrum width the maximum data rate is MCS7 (65Mbps) or MCS15 (130Mbps). If you select 40MHz Channel Spectrum width the maximum data rate is

MCS7 (150Mbps) or MCS15 (300Mbps).

Note: In case you have selected WEP, WPA-TKIP or WPA2-TKIP security method, the maximum data rate is MCS12. This is a hardware limitation due to the Atheros HAL. Should you need a higher data rate try using WPA-AES or WPA2-AES.

Automatic: When the Automatic checkbox is selected, the rate algorithm will select the best data rate, depending on link quality conditions. It is recommended to use the automatic option, especially if you are having trouble getting connected or losing data at a higher rate. Refer to the section *Advanced* for the detailed information about *rate algorithms*.

[Content]

Wireless Security

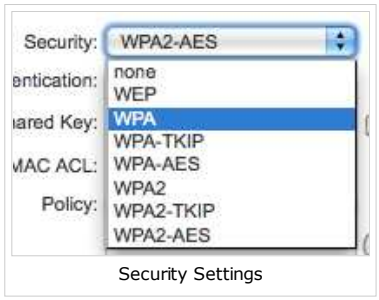
This section enables you to set parameters that control how the subscriber station associates to a wireless device and encrypts/decrypts data.

Wireless Security Settings

Choose the security method according to the Access Point security policy. Subscriber station should be authorized by Access Point in order to get access to the network and all the user data transferred between a subscriber station and Access Point will be encrypted if the wireless security methods are used.

Security: Security: AirOS supports none, WEP, WPA, and WPA2 security options. Select the security mode of your wireless network:

> **WEP** – enable WEP encryption. WEP (Wired Equivalent Privacy) is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. Enabling WEP allows you to increase security by encrypting data being transferred over your wireless network. WEP is the oldest security algorithm, and there are few applications that can decrypt the WEP key in less than 10 minutes. WPA™/WPA2™ security methods should be used when possible.
>
> **WPA** – enable WPA™ security mode. Wi-Fi Protected Access - WPA™ (IEEE 802.11i/D3.0) and WPA2™ (IEEE 802.11i) with pre-shared key management protocol offers improved security methods as they are new protocols that were created under the 802.11i standard to address weaknesses in the WEP approach.



Security Settings

WPA™ and *WPA2*™ support the following ciphers for data encryption:

> **TKIP** - Temporal Key Integrity Protocol that uses RC4 encryption algorithm.
> **AES** (also known as CCMP) - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, which uses the Advanced Encryption Standard (AES) algorithm.

The device will use the strongest cipher (AES) in Station and Access Point wireless mode by default. If AES is not supported on the other side of the link the TKIP encryption will be used - like in situation when the device acts as Access Point with WPA security enabled and at least one wireless station (without AES support) is connected to it.

WPA – enable WPA™ security mode.
WPA-TKIP – enable WPA™ security mode with TKIP support only.
WPA-AES – enable WPA™ security mode with AES support only.
WPA2 – enable WPA2™ security mode.
WPA2-TKIP – enable WPA2™ security mode with TKIP support only.
WPA2-AES – enable WPA2™ security mode with AES support only.

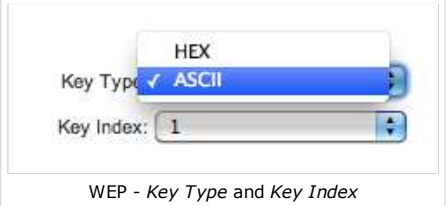
WEP

WEP Security

Authentication Type: field relates **only to the WEP security** option. One of the following authentication modes should be selected if WEP security method is used:

> *Open Authentication* – station is authenticated automatically by AP (selected by default).
> *Shared Authentication* – station is authenticated after the challenge, generated by AP.

WEP Key Length: 64-bit (selected by default) or 128-bit WEP Key length should be selected if WEP security method is used. The *128-bit* option will provide a bit higher level of wireless security.



WEP - *Key Type* and *Key Index*

Key Type: *HEX* (selected by default) or *ASCII* option specifies the character format for the WEP key if WEP security method is used.

WEP Key: WEP encryption key for the wireless traffic encryption and decryption should be specified if WEP security method is used:

> For **64-bit** – specify WEP key as 10 HEX (0-9, A-F or a-f) characters (e.g. 00112233AA) or 5 ASCII characters.
> For **128-bit** – specify WEP key as 26 HEX (0-9, A-F or a-f) characters (e.g. 00112233445566778899AABBCC) or 13 ASCII

characters.

Key Index: allows to specify the Index of the WEP Key used. 4 different WEP keys can be configured at the same time, but only one is used. Effective key is set with a choice of 1, 2, 3 or 4.

WPA/WPA2

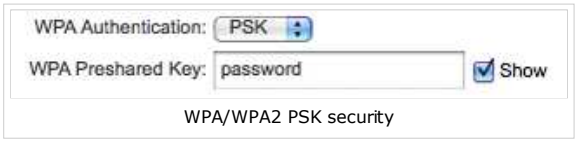
WPA - AES – enable WPA™ security mode with AES support only. Wi-Fi Protected Access - WPA™ (IEEE 802.11i/D3.0) with pre-shared key management protocol offers improved security methods as they are new protocols that were created under the 802.11i standard to address weaknesses in the WEP approach.

WPA2 - AES – enable WPA2™ security mode with AES support only. Wi-Fi Protected Access 2 - WPA2™ (IEEE 802.11i) with pre-shared key management protocol offers improved security methods as they are new protocols that were created under the 802.11i standard to address weaknesses in the WEP approach.

WPA Authentication: one of the following WPA™ key selection methods should be specified if WPA™ or WPA2™ security method is used:

WPA Authentication

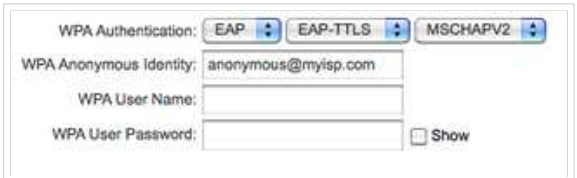
PSK – WPA™ or WPA2™ with Pre-shared Key method (selected by default).
EAP – WPA™ or WPA2™ with EAP (Extensible Authentication Protocol) IEEE 802.1x authentication method. This method is commonly used in Enterprise networks.



WPA/WPA2 PSK security

WPA Pre-shared Key: the pass phrase for WPA™ or WPA2™ security method should be specified if the *Pre-shared Key* method is selected. The pre-shared key is an alpha-numeric password between 8 and 63 characters long.

EAP Authentication - Station Mode



WPA/WPA2 EAP security (Station Mode)

WPA Identity: identification credential (also known as *identity*) used by the supplicant for EAP authentication (applicable to STA and STA WDS modes only).

WPA User Name: identification credential (also known as *anonymous identity*) used by the supplicant for EAP tunneled authentication (EAP-TTLS) in unencrypted form (applicable to STA and STA WDS modes only).

WPA User Password: password credential used by the supplicant for EAP authentication (applicable for STA and STA WDS modes only).

EAP Authentication - AP Mode

WPA/WPA2 EAP security (AP Mode)

Radius Server IP: specifies the RADIUS Server's IP address. RADIUS is a networking protocol providing centralized Authentication, Authorization, and Accounting (AAA) management for computers in order to connect to, and use a network service.

Radius Server Port: specifies the RADIUS Server's UDP port. The most commonly used port is 1812, but that depends on the RADIUS Server you are using.

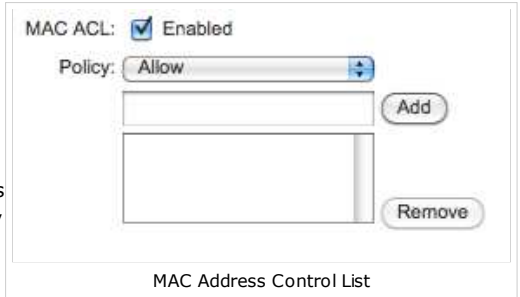
Radius Server Secret: specifies the password. A shared secret is a case-sensitive text string used to validate communications between two RADIUS devices.

Note: When connecting devices in AP-WDS-to-AP-WDS mode, the WPA/WPA2 security methods will not function. When connecting AP-WDS devices to another AP-WDS device use none or the WEP security method. However, this may compromise the security of your network. In case of connecting STA-WDS clients to an AP-WDS device, all security methods are available and work properly.

MAC ACL

The maximum number of MAC ACL entries that can be managed trough the AirOS v5.3 Web GUI is 32 MAC addresses. In order to manage more than 32 entries, read this guide (http://www.ubnt.com/wiki/index.php?title=MAC_ACL_Editing) , which explains how to manage more MAC addresses modifying the configuration file.

MAC ACL: MAC Access Control List (ACL) provides ability to allow or deny certain clients to connect to the AP (applicable to AP and AP WDS modes only).



MAC Address Control List

MAC ACL can be enabled by selecting the **Enabled** checkbox.

There are two ways to set the Access Control List:

define certain wireless clients in the list that will have granted access to the Access Point while the access will be denied for all the remaining clients - MAC ACL **Policy** is set to **Allow'**.
define certain wireless clients in the list that will have denied access to the Access Point while the access will be granted for all the remaining clients - MAC ACL **Policy** is set to **Deny**.

The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Remove** buttons.

Note: MAC Access Control is the weakest security approach. WPA™ or WPA2™ security methods should be used when possible.

Click **Change** button to save the changes.

[Content]

Network

The Network Page allows the administrator to setup bridge or routing functionality.

AirOS v5.3 Network Page

AirOS v5.3 powered devices can operate in bridge, router or SOHO router mode. The IP configuration as described below is required for device management purposes. IP addresses can either be retrieved from a DHCP server or configured manually. Use the *Network* menu to configure the IP settings.

Network Mode: specify the operating network mode for the device. There are three modes: bridge, router and SOHO router. The mode depends on the network topology requirements:

[Bridge] operating mode is selected by default as it is widely used by the subscriber stations, while connecting to Access Point or using WDS. In this mode, the device will act as a transparent bridge and will operate in Layer 2. There will be no network segmentation while broadcast domain will be the same. Bridge mode will not block any broadcast or multicast traffic. Additional *Firewall* settings can be configured for Layer 2 packet filtering and access control in *Bridge* mode.

[Router] operating mode can be configured in order to operate in Layer 3 to perform routing and enable network segmentation – wireless clients will be on different IP subnet. **Router** mode will block broadcasts while it is not transparent.

AirOS v5.3 supports Multicast packet pass-through in **Router** mode.

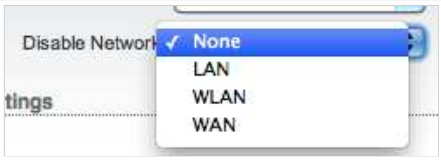
AirOS v5.3 powered *Router* can act as DHCP server and use Network Address Translation (Masquerading) feature, which is widely used by the Access Points. NAT will act as the firewall between LAN and WLAN networks. Additional *Firewall* settings can be configured for Layer 3 packet filtering and access control in *Router* mode.

AirOS Network Mode selection

[SOHO Router]: SOHO (= Small Office and Home Office) Router is basically a derivation from Router mode, which makes the LAN port become the WAN port, and the Wireless network (WLAN) become the local network.

In one-Ethernet-port devices (while operating in AP or AP-WDS) this mode works like the Router mode, except that the LAN port is labeled as "WAN port" and WLAN as LAN. In two-or-more-Ethernet-ports devices, the main Ethernet port becomes WAN, and WLAN and other LAN ports become the local network (LAN).

Disable Network: options can be used for disabling *WLAN*, *LAN* or *WAN* interface. This setting should be used with the exclusive care as no L2 or L3 connection can be established through the disabled interface. It will be impossible to access the AirOS based device from the wireless/wired network that is connected to the disabled interface. *Disable WAN* only applicable while operating in SOHO Router mode.



Disable Network

Network settings

Bridge Mode

In bridge mode the AirOS v5.3 based device forwards all the network management and data packets from one network interface to the other without any intelligent routing. For simple applications this provides an efficient and fully transparent network solution. WLAN (wireless) and LAN (Ethernet) interfaces belong to the same network segment that has the same IP address space. WLAN and LAN interfaces form the virtual *bridge* interface while acting as the *bridge* ports. The *bridge* has assigned IP settings for management purposes:

Bridge mode Network Settings

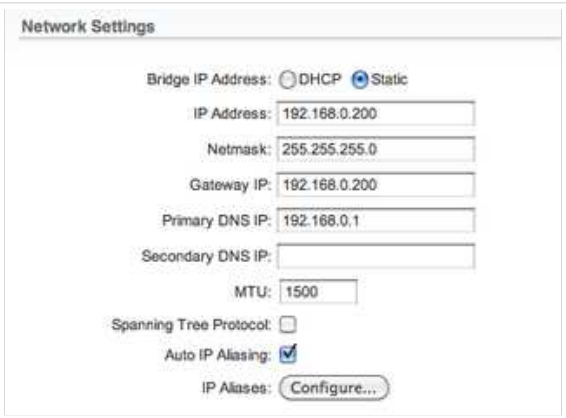
Bridge IP Address: The device can be set for static IP or can be set to obtain an IP address from the DHCP server it is connected to.

One of the IP assignment modes must be selected:

DHCP – choose this option to assign the dynamic IP address, Gateway and DNS address by the local DHCP server.
Static – choose this option to assign the static IP settings for the *bridge* interface.

IP Address: enter the IP address of the device while *Static Bridge IP Address* mode is selected. This IP will be used for the AirOS device management purposes.

IP Address and *Netmask* settings should consist with the address space of the network segment where AirOS v5.3 device resides. If the device IP settings and administrator PC (which is connected to the device in wired or wireless way) IP settings will use different address space, the AirOS device will become unreachable.

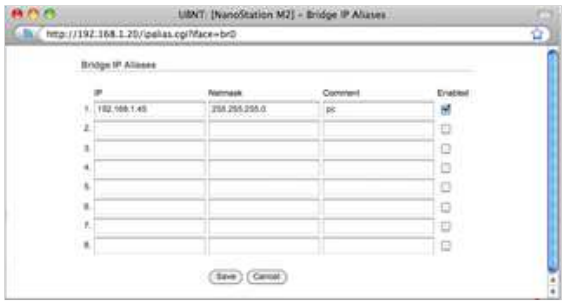


Bridge IP Address assigned manually (Static)

Netmask: This is a value that when expanded into binary provides a mapping to define which portions of IP address groups can be classified as host devices and network devices. Netmask defines the address space of the network segment where AirOS device resides. 255.255.255.0 (or /24) *Netmask* is commonly used among many C Class IP networks.

Gateway IP: Typically, this is the IP address of the host router which provides the point of connection to the internet. This can be a DSL modem, Cable modem, or a WISP gateway router. AirOS v5.3 device will direct the packets of data to the gateway if the destination host is not within the local network.

Gateway IP address should be from the same address space (on the same network segment) as the AirOS device.

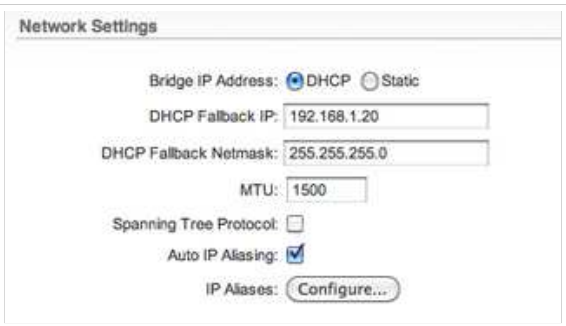

IP Aliases

Primary/Secondary DNS IP: The Domain Name System (DNS) is an internet "phone book", which translates domain names to IP addresses. These fields identify the server IP addresses of where the AirOS device looks for the translation source.

> *Primary DNS* server IP address should be specified for the device management purposes.
>
> *Secondary DNS* server IP address is optional. It is used as the fail-over in case the primary DNS server will become unresponsive.

MTU: defines the size (in bytes) of the largest protocol data unit the layer can pass on. When using slow links, large packets can cause some delays thereby increasing lag and latency

DHCP Fallback IP: In case the *Bridge* is placed in Dynamic IP Address mode (DHCP) and is unable to obtain an IP address from a valid DHCP server, it will fall back to the static IP address listed here.



Bridge IP Address assigned automatically DHCP with IP fallback

In case the IP settings of the AirOS v5.3 powered device are unknown, they can be retrieved with the help of the [UBNT_Discovery_Utility Ubiquiti Discovery Utility]. Multi-platform *Utility* should be started on the administrator PC which resides on the same network segment as the AirOS device.

AirOS v5.3 system will return to the default IP configuration (192.168.1.20/255.255.255.0) If the *Reset to defaults* routine is initiated.

DHCP Fallback Netmask: In case the Bridge is placed in Dynamic IP Address mode (DHCP) and unable to obtain an IP address from a valid DHCP server, it will fall back to the static Netmask listed here.

Spanning Tree Protocol: Multiple interconnected bridges create larger networks using the IEEE 802.1d *Spanning Tree Protocol* (*STP*), which is used for finding the shortest path within the network and to eliminate loops from the topology.

If the *STP* is turned on, the AirOS *Bridge* will communicate with other network devices by sending and receiving *Bridge Protocol Data Units* (BPDU). *STP* should be turned off (selected by default) when the AirOS device is the only bridge on the LAN or when there are no loops in the topology as there is no sense for the *bridge* to participate in the *Spanning Tree Protocol* in this case.

Spanning Tree Protocol enabled

Auto IP Aliasing configures automatically generated *IP Address* for the corresponding WLAN/LAN interface if enabled. Generated IP address is the unique Class B IP address from the 169.254.X.Y (http://en.wikipedia.org/wiki/Link-local_address) range (Netmask 255.255.0.0) which are intended for use within the same network segment only. Auto IP always starts with 169.254.X.Y while X and Y are last 2 digits from device MAC address (i.e. if the MAC is 00:15:6D:A3:04:FB, Generated unique *Auto IP* will be 169.254.4.251).

IP Aliases for internal and external network interface can be configured. *IP Aliases* can be specified using the IP Aliases configuration window that is opened while activating the "Configure" button.

> **IP Address** is the alternative IP address for the LAN or WLAN interface, which can be used for the routing or device management purposes;
> **Netmask** is the network address space identifier for the particular *IP Alias*;
> **Comments** is the informal field for the comment of the particular IP Alias. Few words about the alias purpose are saved there usually;
> **Enabled** flag enables or disables the particular IP Alias. All the added IP Aliases are saved in the system configuration file. However, only the enabled IP Aliases will be active during the AirOS system operation.

Newly added *IP Aliases* can be saved by activating **Save** button or discarded by activating **Cancel** button in the Aliases configuration window.

Click **Change** button to save the changes made in the *Network* page.

Router Mode

The role of the LAN and WLAN interfaces will change accordingly to the **Wireless Mode** while the AirOS powered device is operating, in *Router* mode:

- Wireless interface and all the wireless clients connected are considered as the internal LAN, and the Ethernet interface is dedicated for the connection to the external network while the AirOS powered device is operating in *AP/AP WDS* wireless mode;
- Wireless interface and all the wireless clients connected are considered as the external network, and all the network devices on LAN side as well as the Ethernet interface itself are considered as the internal network while the AirOS powered device is operating in *Station/Station WDS* mode.

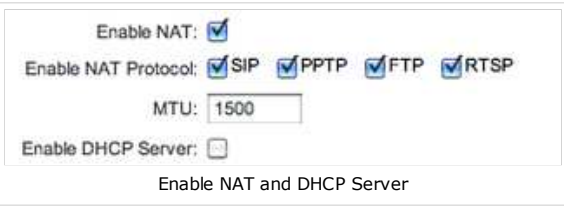
Network - Router mode

Wireless/wired clients are routed from the internal network to the external one by default. Network Address Translation (NAT) functionality works the same way.

WLAN Network Settings

IP Address: This is the IP addresses to be represented by the WLAN interface, which is connected to the internal network according to the wireless operation mode described above. This IP will be used for the routing of the internal network (it will be the *Gateway IP* for all the devices connected on the internal network). This IP address can be used for the management purpose of the AirOS v5.3 powered device.

Netmask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. Class C network *Netmask* uses 24 bits to identify the network (alternative notation "/24") and 8 bits to identity the host.



Enable NAT and DHCP Server

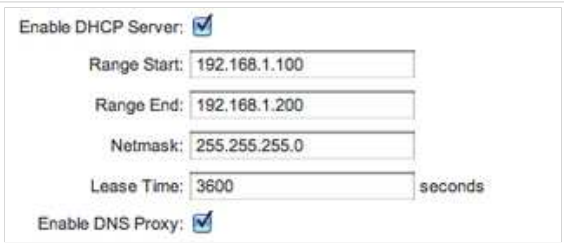
Enable NAT: Network Address Translation (NAT) enables packets to be sent from the wired network (LAN) to the wireless interface IP address and then sub-routed to other client devices residing on its local network while the AirOS powered device is operating in *AP/AP WDS* wireless mode and in the contrariwise direction in "Station/Station WDS" mode.

Enable NAT Protocol: While NAT is enabled, data packets could be modified in order to allow pass-through to the Router. To avoid packets modification of some specific packets, like: SIP, PPTP, FTP, RTSP; uncheck the respective checkbox (-es).

NAT is implemented using the **masquerade** type firewall rules. NAT firewall entries are stored in the iptables *NAT* table, while the device is operating in Router mode. Please refer to the iptables tutorial (http://iptables-tutorial.frozentux.net/iptables-tutorial.html#MASQUERADETARGET) for detailed description of the NAT functionality in *Router* mode.

Static routes should be specified in order the packets should pass-through the AirOS v5.3 based device if the *NAT* is disabled in while operating in *Router* network mode.

Enable DHCP Server: Dynamic Host Configuration Protocol (DHCP) Server assigns IP addresses to clients who will be associate to the wireless interface while the AirOS powered device is operating in *AP/AP WDS* wireless mode and assigns IP addresses to clients who will connect to the LAN interface while the AirOS powered device is operating in *Station/Station WDS* mode.



DHCP Server range, Netmask and lease time

Range Start/End: This range determines the IP addresses given out by the DHCP server to client devices on the internal network that use dynamic IP configuration.

Netmask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. Class C network *Netmask* uses 24 bits to identify the network (alternative notation "/24") and 8 bits to identity the host.

Lease Time: The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interrupt, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more slight interruptions to the client while it will acquire new IP addresses from the DHCP server. The time is expressed in seconds. Maximum lease time value is 172800 seconds.

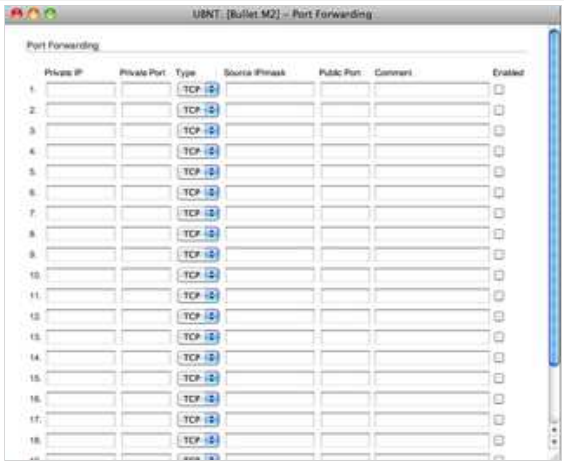
MTU: defines the size (in bytes) of the largest protocol data unit the layer can pass on. When using slow links, large packets can cause some delays thereby increasing lag and latency.

Enable DNS Proxy: The DNS Proxy forwards the Domain Name System requests from the hosts that reside in the internal network to the DNS server while AirOS powered device is in operating in *Router* mode. Valid *Primary DNS Server IP* needs to be specified for *DNS Proxy* functionality. Internal network interface IP of the AirOS powered device should be specified as the DNS server in the host configuration in order *DNS Proxy* should be able to get the DNS requests and translate domain names to IP addresses afterwards.

DNS Proxy and Port Forwarding settings

Port Forwarding: Port forwarding allows specific ports of the hosts residing in the internal network to be forwarded to the external network. This is useful for a number of applications such as FTP servers, gaming, etc. where different host systems need to be seen using a single common IP address/port.

Port Forwarding rules can be set in Port Forwarding window, which is opened by enabling the **Port Forwarding** option and activating the **Configure** button.


Port Forwarding example

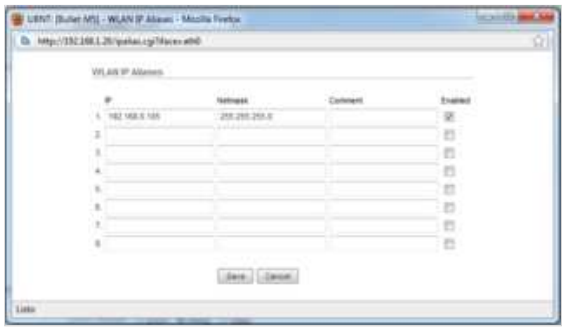
Port Forwarding entries can be specified by using the following criteria:

Private IP is the IP of the host that is connected to the internal network and needs to be accessible from the external network;
Private Port is the TCP/UDP port of the application running on the host that is connected to the internal network. The specified port will be accessible from the external network;
Type is the L3 protocol (IP) type which needs to be forwarded from the internal network.
Public Port is the TCP/UDP port of the AirOS v5.3 based device which will accept and forward the connections from the external network to the host connected to the internal network.
Comments is the informal field for the comment of the particular port forwarding entry. Few words about the particular port forwarding entry purpose are saved there usually.
Enabled flag enables or disables the effect of the particular port forwarding entry. All the added firewall entries are saved in the system configuration file. However, only the enabled port forwarding entries will be active during the AirOS system operation.

Newly added port forwarding entries can be saved by activating **Save** button or discarded by activating **Cancel** button in the *Port Forwarding* configuration window.

Auto IP Aliasing configures automatically generated *IP Address* for the corresponding WLAN/LAN interface if enabled. Generated IP address is the unique Class B IP address from the 169.254.X.Y (http://en.wikipedia.org/wiki/Link-local_address) range (Netmask 255.255.0.0) which are intended for use within the same network segment only. Auto IP always starts with 169.254.X.Y while X and Y are last 2 digits from device MAC address (i.e. if the MAC is 00:15:6D:A3:04:FB, Generated unique *Auto IP* will be 169.254.4.251).

IP Aliases for internal and external network interface can be configured. *IP Aliases* can be specified using the IP Aliases configuration window that is opened while activating the "Configure" button.


IP Aliases

IP Address is the alternative IP address for the LAN or WLAN interface, which can be used for the routing or device management purposes;
Netmask is the network address space identifier for the particular *IP Alias*;
Comments is the informal field for the comment of the particular IP Alias. Few words about the alias purpose are saved there usually;
Enabled flag enables or disables the particular IP Alias. All the added IP Aliases are saved in the system configuration file. However, only the enabled IP Aliases will be active during the AirOS system operation.

Newly added *IP Aliases* can be saved by activating **Save** button or discarded by activating **Cancel** button in the Aliases configuration window.

LAN Network Settings

LAN IP Address: This is the IP addresses to be represented by the LAN or WLAN interface that is connected to the external network according to the wireless operation mode described above. This is the IP address can be used for the routing and the device management purposes.

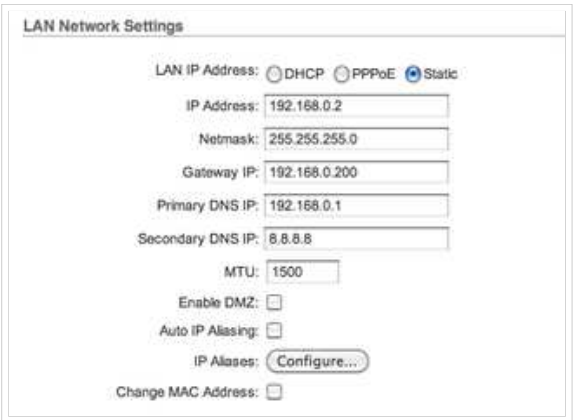
The external network interface can be set for static IP or can be set to obtain an IP address from the DHCP server, which should reside in the external network. One of the IP assignment modes must be selected for the external network interface:

DHCP – choose this option to obtain the IP address, Gateway and DNS address dynamically from the external DHCP server.
PPPoE – choose this option to obtain the IP address, Gateway and DNS address dynamically from the external PPPoE server.
Static – choose this option to assign the static IP settings for the external interface.

IP Address and *Netmask* settings should consist with the address space of the network segment where AirOS device resides. If the device IP settings and administrator PC (which is connected to the device in wired or wireless way) IP settings will use different address space, the AirOS device will become unreachable. (Applicable for Static mode only)

Netmask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. Class C network *Netmask* uses 24 bits to identify the network (alternative notation "/24") and 8 bits to identity the host. (Applicable for Static mode only)

Gateway IP: is the IP address of the host router that resides on the external network and provides the point of connection to the next hop towards the internet. This can be a DSL modem, Cable modem, or a WISP gateway router. AirOS device will direct all the packets to the gateway if the destination host is not within the local network. (Applicable for Static mode only)



LAN IP Address assigned manually - Static

Gateway IP address should be from the same address space (on the same network segment) as the AirOS device's external network interface (Wireless interface in the *Station* case and the LAN interface in the *AP* case). (Applicable for Static mode only)

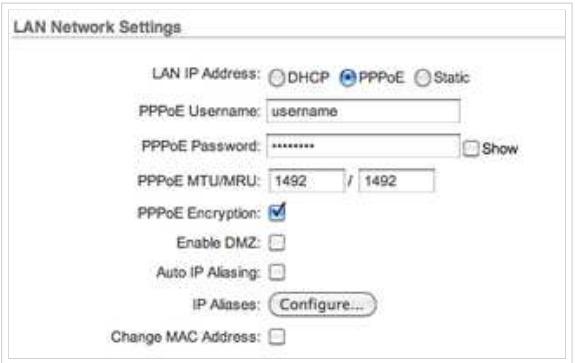
Primary/Secondary DNS IP: The Domain Name System (DNS) is an internet "phone book", which translates domain names to IP addresses. These fields identify the server IP addresses where the DNS requests are forwarded by the AirOS v5.3 powered device. (Applicable for Static mode only)

Primary DNS server IP is mandatory. It is used by the *DNS Proxy* and for the device management purpose.

Secondary DNS server IP address is optional. It is used as the fail-over in case the primary DNS server will become unresponsive.

PPPoE: Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection between two systems, which enables encapsulated data transport. It is commonly used as the medium for subscribers to connect to Internet Service Providers.

Select the IP Address option *PPPoE* to configure a PPPoE tunnel in order to connect to an ISP. Only the external network interface can be configured as PPPoE client as all the traffic will be sent via this tunnel. The IP address, Default gateway IP and DNS server IP address will be obtained from the PPPoE server after PPPoE connection is established. Broadcast address is used for the PPPoE server discovery and tunnel establishment.



PPPoE Internet connection (usually used by ADSL providers)

Valid authorization credentials are required for the PPPoE connection:

PPPoE Username – username to connect to the server (must match the configured on the PPPoE server);
PPPoE Password – password to connect to the server (must match the configured on the PPPoE server);
Show: Check this box to display the PPPoE password characters.

PPPoE MTU/MRU – the size (in bytes) of the Maximum Transmission Unit (MTU (http://en.wikipedia.org /wiki/Maximum_transmission_unit)) and Maximum Receive Unit (MRU) used for the data encapsulation while transferring it through the PPP (http://tools.ietf.org/html/rfc1661) tunnel; (MTU/MRU default value: 1492)
PPPoE Encryption – enables the use of MPPE encryption.

IP address of the PPP interface will be displayed in the *Main* page next to the PPP interface statistics if it is obtained through the established PPPoE connection, otherwise "Not Connected" message will be displayed.

PPPoE tunnel reconnection routine can be initiated using the *Reconnect* button, which is located in the *Main* page next to the PPP interface statistics.

Enable DMZ: The Demilitarized zone (DMZ) can be enabled and used as a place where services can be placed such as Web Servers, Proxy Servers, and E-mail Servers such that these services can still serve the local network and are at the same time isolated from it for additional security. *DMZ* is commonly used with the *NAT* functionality as an alternative for the *Port Forwarding* while makes all the ports of the host network device be visible from the external network side.

DMZ Management Port: Web Management Port for the AirOS v5.3 based device (TCP/IP port 80 by default) will be used for the host device if *DMZ Management Port* option is enabled. In this case AirOS device will respond to the requests from the external network as if it was the host that is specified with *DMZ IP*. It is recommended to leave *Management Port* disabled while the AirOS based device will become inaccessible from the external network if enabled.

DMZ configuration

DMZ IP: connected to the internal network host, specified with the *DMZ IP* address will be accessible from the external network.

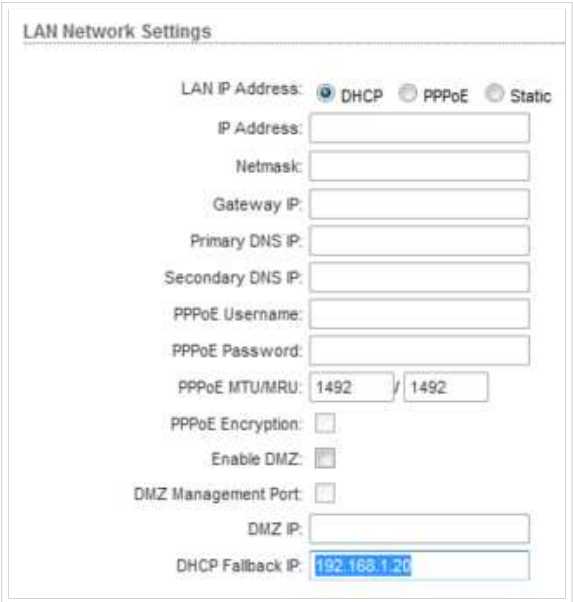
DHCP Fallback IP: In case the external network interface of the *Router* is placed in Dynamic IP Address mode (DHCP) and is unable to obtain an IP address from a valid DHCP server, it will fall back to the static IP address listed here.

DHCP Fallback Netmask: In case the Router is placed in Dynamic IP Address mode (DHCP) and unable to obtain an IP address from a valid DHCP server, it will fall back to the static Netmask listed here.

In case the IP settings of the AirOS powered device are unknown, they can be retrieved with the help of the [UBNT_Discovery_Utility Ubiquiti Discovery Utility]. Multi-platform *Utility* should be started on the administrator PC, which resides on the same network segment as the AirOS device.

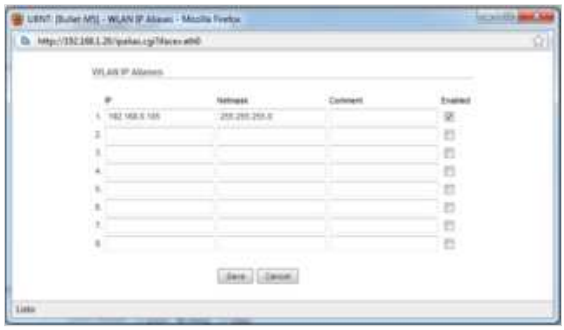
AirOS v5.3 system will return to the default IP configuration (192.168.1.20/255.255.255.0) if the *Reset to defaults* routine is initiated (more information in System section).

Auto IP Aliasing configures automatically generated *IP Address* for the corresponding WLAN/LAN interface if enabled. Generated IP address is the unique Class B IP address from the 169.254.X.Y (http://en.wikipedia.org/wiki/Link-local_address) range (Netmask 255.255.0.0), which are intended for use within the same network segment only. Auto IP always starts with 169.254.X.Y while X and Y are last 2 digits from device MAC address (i.e. if the MAC is 00:15:6D:A3:04:FB, Generated unique *Auto IP* will be 169.254.4.251).



LAN IP Address assigned via DHCP with IP fallback

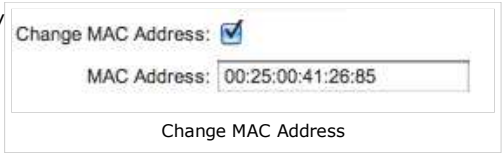
IP Aliases for internal and external network interface can be configured. *IP Aliases* can be specified using the IP Aliases configuration window that is opened while activating the "Configure" button.


IP Aliases

- **IP Address** is the alternative IP address for the LAN or WLAN interface, which can be used for the routing or device management purposes;
- **Netmask** is the network address space identifier for the particular *IP Alias*;
- **Comments** is the informal field for the comment of the particular IP Alias. Few words about the alias purpose are saved there usually;
- **Enabled** flag enables or disables the particular IP Alias. All the added IP Aliases are saved in the system configuration file. However, only the enabled IP Aliases will be active during the AirOS system operation.

Newly added *IP Aliases* can be saved by activating **Save** button or discarded by activating **Cancel** button in the Aliases configuration window.

Change MAC Address: When checked, the MAC address of the respective interface may be changed easily. This is especially useful if your ISP only assigns one valid IP address associated to a specific MAC address; usually used by Cable operators or some WISP.



Change MAC Address

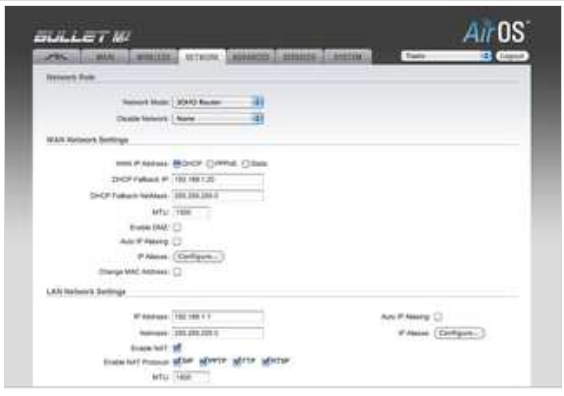
SOHO Router

SOHO (= Small Office and Home Office) Router is basically a derivation from Router mode, which makes the LAN port become the WAN port, and the Wireless network (WLAN) become the local network.

SOHO router mode only works properly in AP or AP-WDS modes, since it has not been designed to acts as a wireless client.

In one-Ethernet-port devices (while operating in AP or AP-WDS) this mode works like the Router mode, except that the LAN port is labeled as "WAN port" and WLAN as LAN. In two-or-more-Ethernet-ports devices, the main Ethernet port becomes WAN, and WLAN and other LAN ports become the local network (LAN).

Note: Don't use the SOHO Router mode in combination with Station or Station WDS wireless mode on one-Ethernet-port devices; it may cause the device to become not accessible. In such a case, reset the device to defaults values by pressing the Reset button for 8 seconds and then releases it.



Network - SOHO Router mode

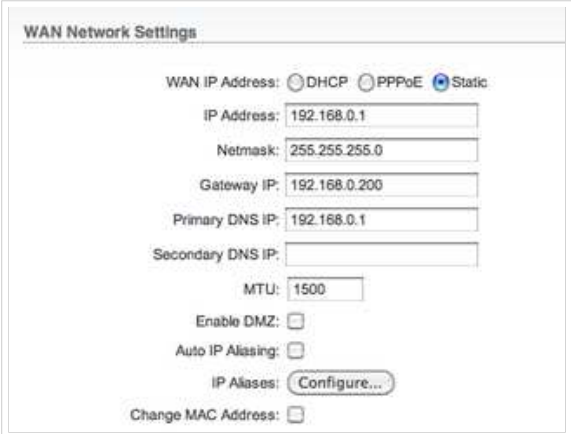
WAN Network Settings

'*WAN IP Address*: This is the IP address to be represented by the WAN interface, which is connected to the external network. This is the IP address can be used for the routing and the device management purposes.

The WAN interface can be set for static IP or can be set to obtain an IP address from the DHCP server, which should reside in the external network. One of the IP assignment modes must be selected for the external network interface:

- **DHCP** – choose this option to obtain the IP address, Gateway and DNS address dynamically from the external DHCP server.
- **PPPoE** – choose this option to obtain the IP address, Gateway and DNS address dynamically from the external PPPoE server.

Static – choose this option to assign the static IP settings for the external interface.



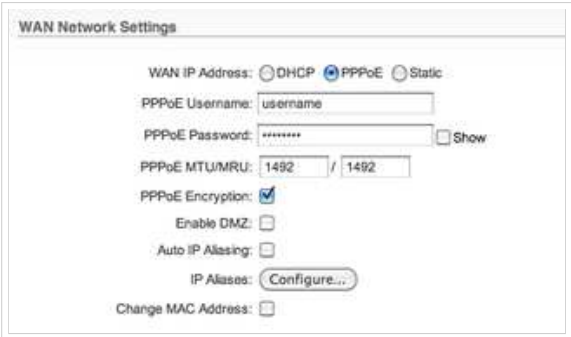
WAN IP Address assigned manually - Static

Netmask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. Class C network Netmask uses 24 bits to identify the network (alternative notation "/24") and 8 bits to identity the host.

Gateway IP: is the IP address of the host router that resides on the external network and provides the point of connection to the next hop towards the internet. This can be a DSL modem, Cable modem, or a WISP gateway router. AirOS v5.3 device will direct all the packets to the gateway if the destination host is not within the local network.

Primary/Secondary DNS IP: The Domain Name System (DNS) is an internet "phone book", which translates domain names to IP addresses. These fields identify the server IP addresses where the DNS requests are forwarded by the AirOS powered device.

MTU: defines the size (in bytes) of the largest protocol data unit the layer can pass on. When using slow links, large packets can cause some delays thereby increasing lag and latency



PPPoE Internet connection (usually used by ADSL providers)

PPPoE: Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection between two systems that enables encapsulated data transport. It is commonly used as the medium for subscribers to connect to Internet Service Providers (ISP).

Select the IP Address option *PPPoE* to configure a PPPoE tunnel in order to connect to an ISP. Only the WAN interface can be configured as PPPoE client as all the traffic will be sent via this tunnel. The IP address, Default gateway IP and DNS server IP address will be obtained from the PPPoE server after PPPoE connection is established. Broadcast address is used for the PPPoE server discovery and tunnel establishment.

Valid authorization credentials are required for the PPPoE connection:

PPPoE Username – username to connect to the server (must match the configured on the PPPoE server);
PPPoE Password – password to connect to the server (must match the configured on the PPPoE server);
Show: Check this box to display the PPPoE password characters.

PPPoE MTU/MRU – the size (in bytes) of the Maximum Transmission Unit (MTU (http://en.wikipedia.org/wiki/Maximum_transmission_unit)) and Maximum Receive Unit (MRU) used for the data encapsulation while transferring it through the PPP (http://tools.ietf.org/html/rfc1661) tunnel; (MTU/MRU default value: 1492)
PPPoE Encryption – enables the use of MPPE encryption.

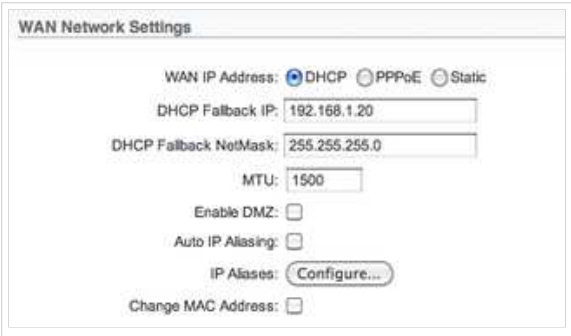
IP address of the PPP interface will be displayed in the *Main* page next to the PPP interface statistics if it is obtained through the established PPPoE connection, otherwise "Not Connected" message will be displayed.

PPPoE tunnel reconnection routine can be initiated using the *Reconnect* button, which is located in the *Main* page next to the PPP interface statistics.

Enable DMZ: The Demilitarized Zone (DMZ) can be enabled and used as a place where services can be placed such as Web Servers, Proxy Servers, and E-mail Servers such that these services can still serve the local network and are at the same time isolated from it for additional security. DMZ is commonly used with the NAT functionality as an alternative for the Port Forwarding while makes all the ports of the host network device be visible from the external network side.

DMZ Management Port: Web Management Port for the AirOS v5.3 based device (TCP/IP port 80 by default) will be used for the host device if DMZ Management Port option is enabled. In this case AirOS device will respond to the requests from the external network as if it was the host that is specified with DMZ IP. It is recommended to leave Management Port disabled while the AirOS based device will become inaccessible from the external network if enabled.

DMZ IP: connected to the internal network host, specified with the DMZ IP address will be accessible from the external network.



WAN IP Address assigned via DHCP with IP fallback

DHCP Fallback IP: In case the WAN interface of the *SOHO Router* is placed in Dynamic IP Address mode (DHCP) and is unable to obtain an IP address from a valid DHCP server, it will fall back to the static IP address listed here.

DHCP Fallback Netmask: In case the Router is placed in Dynamic IP Address mode (DHCP) and unable to obtain an IP address from a valid DHCP server, it will fall back to the static Netmask listed here.

Auto IP Aliasing: configures automatically generated IP Address for the corresponding WAN/WLAN-LAN interface if enabled. Generated IP address is the unique Class B IP address from the 169.254.X.Y range (Netmask 255.255.0.0) that are intended for use within the same network segment only. Auto IP always starts with 169.254.X.Y while X and Y are last 2 digits from device MAC address

(i.e. if the MAC is 00:15:6D:A3:04:FB, Generated unique Auto IP will be 169.254.4.251).

IP Aliases: for internal and external network interface can be configured. IP Aliases can be specified using the IP Aliases configuration window that is opened while activating the "Configure" button.

IP Address is the alternative IP address for the LAN or WLAN interface, which can be used for the routing or device management purposes;
Netmask is the network address space identifier for the particular IP Alias;
Comments is the informal field for the comment of the particular IP Alias. Few words about the alias purpose are saved there usually;
Enabled flag enables or disables the particular IP Alias. All the added IP Aliases are saved in the system configuration file. However, only the enabled IP Aliases will be active during the AirOS system operation.

Change MAC Address: When checked, the MAC address of the respective interface may be changed easily. This is especially useful if your ISP only assigns one valid IP address associated to a specific MAC address; usually used by Cable operators or some WISP.

LAN Network Settings

IP Address: This is the IP addresses to be represented by the LAN (including WLAN) interface that is connected to the internal network. This IP will be used for the routing of the internal network (it will be the *Gateway IP* for all the devices connected on the internal network). This is the IP address can be used for the management purpose of the AirOS v5.3 powered device.

Netmask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. Class C network *Netmask* uses 24 bits to identify the network (alternative notation "/24") and 8 bits to identity the host.

Enable NAT: Network Address Translation (NAT) enables packets to be sent from the external network (WAN) to the local interface IP address and then sub-routed to other client devices residing on it's local network while the AirOS powered device is operating in *AP/AP WDS* wireless mode.

Enable NAT

Enable NAT Protocol: While NAT is enabled, data packets could be modified in order to allow pass-through to the Router. To avoid packets modification of some specific packets, like: SIP, PPTP, FTP, RTSP; uncheck the respective checkbox (-es).

NAT is implemented using the **masquerade** type firewall rules. NAT firewall entries are stored in the iptables *nat* table, while the device is operating in Router mode. Please refer to the iptables tutorial (http://iptables-tutorial.frozentux.net/iptables-tutorial.html#MASQUERADETARGET) for detailed description of the NAT functionality in *Router* mode.

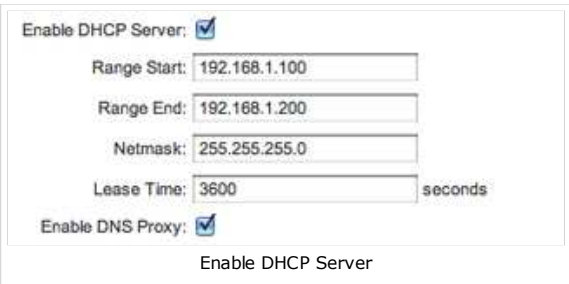
Static routes should be specified in order the packets should pass-through the AirOS v5.3 based device if the *NAT* is disabled in while operating in *SOHO Router* network mode.

MTU: defines the size (in bytes) of the largest protocol data unit the layer can pass on. When using slow links, large packets can cause some delays thereby increasing lag and latency.

Enable DHCP Server: Dynamic Host Configuration Protocol (DHCP) Server assigns IP addresses to clients that will associate to the wireless interface while the AirOS powered device is operating in *AP/AP WDS* wireless mode and assigns IP addresses to clients, which will connect to the LAN interface while the AirOS powered device is operating in *Station/Station WDS* mode.

Range Start/End: This range determines the IP addresses given out by the DHCP server to client devices on the internal network that use dynamic IP configuration.

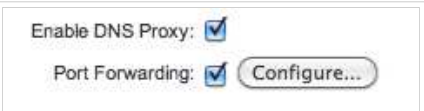
Netmask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. Class C network *Netmask* uses 24 bits to identify the network (alternative notation "/24") and 8 bits to identity the host.



Enable DHCP Server

Lease Time: The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interrupt, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more slight interruptions to the client while it will acquire new IP addresses from the DHCP server. The time is expressed in seconds.

Enable DNS Proxy: The DNS Proxy forwards the Domain Name System requests from the hosts that reside in the internal network to the DNS server while AirOS powered device is in operating in *SOHO Router* mode. Valid *Primary DNS Server IP* needs to be specified for *DNS Proxy* functionality. Internal network interface IP of the AirOS powered device should be specified as the DNS server in the host configuration in order *DNS Proxy* should be able to get the DNS requests and translate domain names to IP addresses afterwards.



DNS Proxy and Port Forwarding settings

Port Forwarding: Port forwarding allows specific ports of the hosts residing in the internal network to be forwarded to the external network (WAN). This is useful for number of applications such as FTP servers, voip, gaming, etc. where different host systems need to be seen using a single common IP address/port.

Port Forwarding rules can be set in Port Forwarding window, which is opened by enabling the **Port Forwarding** option and activating the **Configure** button.

Port Forwarding entries can be specified by using the following criteria:

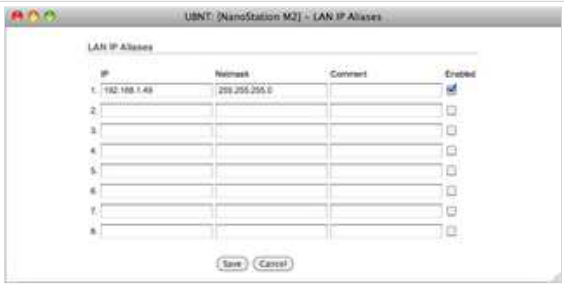
Private IP is the IP of the host that is connected to the internal network and needs to be accessible from the external network;
Private Port is the TCP/UDP port of the application running on the host that is connected to the internal network. The specified port will be accessible from the external network;
Type is the L3 protocol (IP) type that need to be forwarded from the internal network.
Public Port is the TCP/UDP port of the AirOS v5.3 based device that will accept and forward the connections from the external network to the host connected to the internal network.
Comments is the informal field for the comment of the particular port forwarding entry. Few words about the particular port forwarding entry purpose are saved there usually.

Enabled flag enables or disables the effect of the particular port forwarding entry. All the added firewall entries are saved in the system configuration file. However, only the enabled port forwarding entries will be active during the AirOS system operation.

Newly added port forwarding entries can be saved by activating **Save** button or discarded by activating **Cancel** button in the *Port Forwarding* configuration window.

Auto IP Aliasing configures automatically generated *IP Address* for the corresponding WAN/LAN interface if enabled. Generated IP address is the unique Class B IP address from the 169.254.X.Y (http://en.wikipedia.org/wiki/Link-local_address) range (Netmask 255.255.0.0), which are intended for use within the same network segment only. Auto IP always starts with 169.254.X.Y while X and Y are last 2 digits from device MAC address (i.e. if the MAC is 00:15:6D:A3:04:FB, Generated unique *Auto IP* will be 169.254.4.251).

IP Aliases for internal and external network interface can be configured. *IP Aliases* can be specified using the IP Aliases configuration window that is opened while activating the "Configure" button.



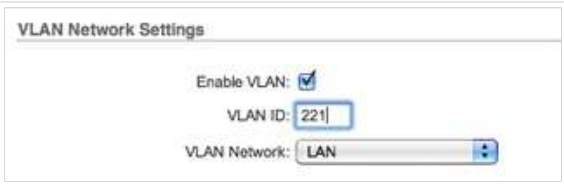
IP Aliases

IP Address is the alternative IP address for the LAN or WLAN interface, which can be used for the routing or device management purposes;
Netmask is the network address space identifier for the particular *IP Alias*;
Comments is the informal field for the comment of the particular IP Alias. Few words about the alias purpose are saved there usually;
Enabled flag enables or disables the particular IP Alias. All the added IP Aliases are saved in the system configuration file. However, only the enabled IP Aliases will be active during the AirOS system operation.

Newly added *IP Aliases* can be saved by activating **Save** button or discarded by activating **Cancel** button in the Aliases configuration window.

VLAN Network Settings

Enable VLAN: defines the size (in bytes) of the largest protocol data unit the layer can pass on. When using slow links, large packets can cause some delays thereby increasing lag and latency.



VLAN Network Settings

VLAN ID: The VLAN ID is a unique value assigned to each VLAN at a single device; every VLAN ID represents a different Virtual Network. In AirOS 5.3 VLAN ID range values between 2 and 4094 are allowed. AirOS 5.3 only allows for one VLAN ID per device.

VLAN Network: defines which network interface will be assigned to the specified VLAN ID.

Multicast Routing Settings

With a multicast design, applications can send one copy of each packet and address it to the group of computers that want to receive it. This technique addresses packets to a group of receivers rather than to a single receiver. It depends on the network to forward the packets to the hosts that need to receive them. Common Routers isolate all the broadcast (thus multicast) traffic between the internal and external networks, however AirOS provides the multicast traffic pass-through functionality.

Enable Multicast Routing option enables the multicast packets pass-through between internal and external networks while device is operating in *Router* mode. Multicast intercommunication is based on Internet Group Management Protocol (IGMP) (http://en.wikipedia.org/wiki/Internet_Group_Management_Protocol) .

Multicast routing enabled and Multicast Upstream

Multicast Upstream: specify the source of Multicast traffic, i.e. defines where multicast traffic comes from.

Firewall Settings

Firewall functionality on any router interface can be enabled using the "Enable Firewall" option. Router Firewall rules can be configured, enabled or disabled while using Firewall configuration window that is opened with the "Configure" button.

Firewall Configuration Settings

Firewall entries can be specified by using the following criteria:

Action allows two specific firewall rules: ACCEPT or DROP. By enabling "Accept", the packets can pass the firewall unmodified. When choosing "DROP", the packets are denied passage through the firewall and no response is sent.
Interface the interface (WLAN, LAN or PPP) where filtering of the incoming/passing-through packets is processed;
IP Type sets which particular L3 protocol type (IP, ICMP, TCP, UDP, P2P) should be filtered;
Source IP/mask is the source IP of the packet (specified within the packet header), usually it is the IP of the host system that sends the packets;
Source Port is the source port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application that sends the packets;
Destination IP/mask is the destination IP of the packet (specified within the packet header), usually it is the IP of the system which the packet is addressed to;
Destination Port is the destination port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which the packet is addressed to.
Comments is the informal field for the comment of the particular firewall entry. Few words about the particular firewall entry purpose are saved there usually.
On flag enables or disables the effect of the particular firewall entry. All the added firewall entries are saved in system configuration file, however only the enabled firewall entries will be active during the AirOS system operation.
Not operators can be used for inverting the *Source IP/mask*, *Source Port*, *Destination IP/mask* and *Destination Port* filtering criteria (i.e. if *not* is enabled for the specified *Destination Port* value 443, the filtering criteria will be applied to all the packets sent to any *Destination Port* except the 443, which is commonly used by HTTPS).

Newly added *Firewall* entries can be saved by activating **Save** button or discarded by activating **Cancel** button in the Firewall configuration window.

Static Routes

All the active firewall entries are stored in the FIREWALL chain of the *iptables filter* table, while the device is operating in Router mode. Please refer to the iptables tutorial (http://iptables-tutorial.frozentux.net/iptables-tutorial.html) for detailed description of the firewall functionality in *Router* mode.

Click Change button to save the changes made in the Network page.

Static Routes

In this section, you can manually add static routing rules to the System Routing Table, this allows you to specify that a specific target IP address (es) passes through a determined gateway.

For each entry, you must specify a valid *Target Network IP, Netmask, Gateway IP, and optionally a comment*, and check the "ON" checkbox, in order to enable this rule. Finally press "Save" button to apply changes or "Cancel" to discard them.

[Content]

Advanced

This page handles advanced routing and wireless settings. The Advanced options page allows you to manage advanced settings that influence on the device performance and behavior. The advanced wireless settings are dedicated for more technically advanced users who have a sufficient knowledge about wireless LAN technology. These settings should not be changed; unless you know what effect the changes will have on your device.

Advanced Wireless Settings in BulletM2

Advanced Wireless Setting

The 802.11n data rates include MCS0, MCS1, MCS2, MCS3, MCS4, MCS5, MCS6, MCS7 for 1x1 chain devices and MCS8, MCS9, MCS10, MCS11, MCS12, MCS13, MCS, MCS15 for 2x2 chains devices. The ACK timeout has a critical impact on performance in 802.11n outdoor links.

RTS Threshold: determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The range is 0-2346bytes, or word "off". The default value is 2346, which means that RTS is disabled.

RTS and Fragmentation Threshold

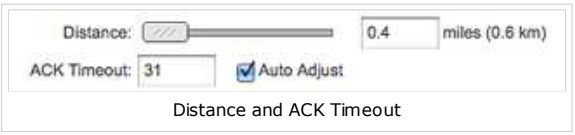
RTS/CTS (Request to Send / Clear to Send) are the mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden terminal problem. RTS/CTS packet size threshold is 0-2346 bytes. If the packet size the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. If the packet size is equal to or less than threshold the data frame gets sent immediately.

System uses Request to Send/Clear to Send frames for the handshake that provide collision reduction for an access point with hidden stations. The stations are sending a RTS frame first while data is sent only after a handshake with an AP is completed. Stations respond with the CTS frame to the RTS, which provides clear media for the requesting station to send the data. CTS collision control management has a time interval defined during which all the other stations hold off the transmission and wait until the requesting station will finish transmission.

Fragmentation Threshold: specifies the maximum size for a packet before data is fragmented into multiple packets. The range is 256-2346 bytes, or word "off". Setting the *Fragmentation Threshold* too low may result in poor network performance.

The use of fragmentation can increase the reliability of frame transmissions. Because of sending smaller frames, collisions are much less likely to occur. However, lower values of the *Fragmentation Threshold* will result in lower throughput as well. Minor or no modifications of the *Fragmentation Threshold* value is recommended while default setting of 2346 is optimum in most of the wireless network use cases.

AirOS v5.3 has a new auto-acknowledgement timeout algorithm, which dynamically optimizes the frame acknowledgement timeout value without user intervention. This is a critical feature required for stabilizing long-distance 802.11n outdoor links. The user also has the ability to enter the value manually, but it's not recommended.



Distance and ACK Timeout

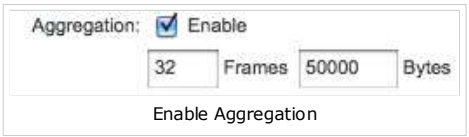
Distance: specify the distance value in miles (or kilometers) using slider or enter the value manually. The signal strength and throughput falls off with range. Changing the distance value will change the ACK Timeout to the appropriate value of the distance.

ACK Timeout: specify the *ACK Timeout*. Every time the station receives the data frame it sends an ACK frame to the AP (if transmission errors are absent). If the station receives no ACK frame from the AP within set *timeout* it re-sends the frame. The performance drops because of the too many data frames are re-send, thus if the *timeout* is set too short or too long, it will result in poor connection and throughput performance.

Changing the *ACK Timeout''* value will change the *Distance* to the appropriate distance value for the ACK Timeout.

Auto Adjust control will enable the ACK Timeout Self-Configuration feature. If enabled, ACK Timeout value will be derived dynamically using an algorithm similar to the Conservative Rate Algorithm (used in AirOS v3.4). It is very recommended to use *Auto Adjust* option for 802.11n.

If two or more stations are located at the considerably different distance from the Access Point are associated to, the highest *ACK Timeout* for the farthest station should be set at the AP side. AirOS v5.3 includes an improved ACK Timeout algorithm.



Enable Aggregation

Aggregation: A part of the 802.11n standard (or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.

Frames – determines the number of frames combined on the new larger frame.

Bytes – determines the size (in Bytes) of the larger frame.

Multicast Data: This option allows all the Multicast packet pass-through functionality. By default this option is disabled.

Enable Multicast and Extra Reporting

Enable Extra Reporting: feature will report additional information (i.e. Host Name) in the 802.11 management frames. This information is commonly used for system identification and status reporting in discovery utilities and Router operating systems.

Enable DFS

Enable DFS: *DFS* is the part of the IEEE 802.11h wireless standard. *Enable DFS* option allows to enable/disable DFS support (applicable to M5 series only). DFS may be mandatory in some regulatory domains and should be tuned according to the regulations of the selected country. Please consult compliance guide (http://www.ubnt.com/wiki/RF_Compliance) and official regulations authorities for further explanation of compliance requirements for the country where AirOS v5.3 based device is installed.

Sensitivity Threshold

Enable Client Isolation: This option allows packets only to be sent from the external network to the CPE and vice verse (applicable for *AP/AP WDS* mode only). If the *Client Isolation* is enabled wireless stations connected to the same AP will not be able to interconnect on both layer 2 (MAC) and layer 3 (IP) level. This is effective for the associated stations and WDS peers also.

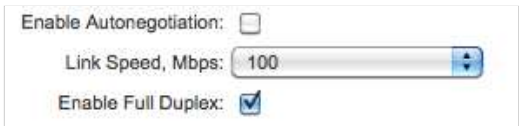
Sensitivity Threshold, dBm: defines the minimum client signal level accepted by the AP, for the client to remain associated. Any client with a signal level lower than that specified will be kicked out. Actually, this feature is helpful to maintain good signal levels within the stations associated, assuring better overall performance. Unchecking the OFF checkbox disables the feature.

Advanced Ethernet Settings

Enable PoE Passthrough: (only applies to Nano M-series): when enabled, the device allows to pass POE's power from Main Port to the secondary port, thereby allowing to feed a further device, like a compatible IP camera.

Enable PoE Passthrough

Enable Autonegotiation: When enabled, the device will automatically negotiate transmission parameters with the counterpart, such as speed and duplex. In this process, the connected devices first share their capabilities as for these parameters and then choose the fastest transmission mode they both support. In case you want to specify these values manually disable Autonegotitation option and select the proper values bellow:



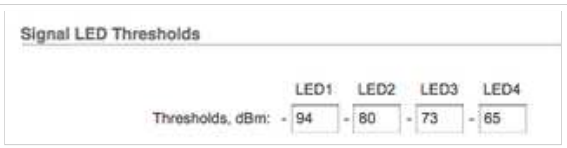
Ethernet Negotiation

Link Speed, Mbps: selects the maximum transmission link speed. There are two options: 10Mbps or 100Mbps. If running extra long Ethernet cables, a link speed of 10Mbps could help to achieve better stability.

Enable Full Duplex: selects the duplex mode; if enabled, the device operates in Full Duplex (allowing bidirectional communication in both directions simultaneously). While disabled, the device operates in Half-Duplex mode (allowing bidirectional communication in both directions, but not simultaneously and only in one direction at a time.

Signal LED Thresholds

The LED's on the back of the AirOS v5.3 Device can be made to light on when received signal levels reach the values defined in the following fields. This allows a technician to easily deploy an AirOS CPE without logging into the unit (i.e. for antenna alignment operation).



LED Thresholds Configuration

Signal LED Thresholds specify the marginal value of Signal Strength (dBm), which will switch on LEDs indicating signal strength:

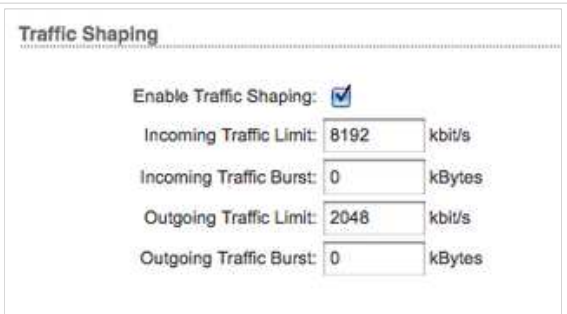
- **LED 1** (Red) will switch on if the Signal Strength reaches the value set in an entry field next to it. The default value is -94dBm.
- **LED 2** (Yellow) will switch on if the Signal Strength reaches the value set in an entry field next to it. The default value is -80dBm.
- **LED 3** (Green) will switch on if the Signal Strength reaches the value set in an entry field next to it. The default value is -73dBm.
- **LED 4** (Green) will switch on if the Signal Strength reaches the value set in an entry field next to it. The default value is -65dBm.

Configuration example: if the Signal Strength (displayed in the *Main* page) fluctuates around -63 dBm, the LED Thresholds can be set to the values -70, -65, -62, -60. **Note: sign "-" character should not be used for the Signal Strength value specification**.

Traffic Shaping

Wireless Traffic shaping feature is dedicated for upstream and downstream bandwidth control while looking from the client (connected on Ethernet interface) perspective.

The traffic can be limited at the AirOS based device in the upload and download direction based on a user defined rate limit. This is layer 3 QoS.


Traffic Shaping
Enable Traffic Shaping:
Incoming Traffic Limit: 8192 kbit/s
Incoming Traffic Burst: 0 kBytes
Outgoing Traffic Limit: 2048 kbit/s
Outgoing Traffic Burst: 0 kBytes
Wireless Traffic Shapping

Enable Traffic Shaping: control will enable bandwidth control on the device.

Incoming Traffic Limit: specify the maximum bandwidth value (in kilobits per second, Kbps) for traffic passing from wireless interface to Ethernet interface.

Incoming Traffic Burst: specify the data volume (in kilobytes) to which *Incoming Traffic Limit* will not be effective afterwards data connection is initiated.

Outgoing Traffic Limit: specify the maximum bandwidth value (in kilobits per second, Kbps) for traffic passing from Ethernet interface to wireless interface.

Outgoing Traffic Burst: specify the data volume (in kilobytes) to which *Outgoing Traffic Limit* will not be effective afterwards data connection is initiated.

[Content]

Services

This page covers the configuration of system management services SNMP, SSH, System Log and Ping Watchdog.

Ping WatchDog

Services Page

The ping watchdog sets the AirOS v5.3 Device to continuously ping a user-defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, the AirOS device will automatically reboot. This option creates a kind of "fail-proof" mechanism.

Ping Watchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP "echo request" packets to the target host and listening for ICMP "echo response" replies. If the defined number of replies is not received, the tool reboots the device.

Enable Ping Watchdog: control will enable Ping Watchdog Tool.

IP Address To Ping: specify an IP address of the target host which will be monitored by Ping Watchdog Tool.

Ping Interval: specify time interval (in seconds) between the ICMP "echo requests" are sent by the Ping Watchdog Tool. The default value is 300 seconds.

Startup Delay: specify initial time delay (in seconds) until first ICMP "echo request" is sent by the Ping Watchdog Tool. The default value is 300 seconds.

Ping Watchdog

The value of Startup Delay should be at least 60 seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted.

Failure Count to Reboot: specify the number of ICMP "echo response" replies. If the specified number of ICMP "echo response" packets is not received continuously, the Ping Watchdog Tool will reboot the device. The default value is 3.

SNMP Agent

Simple Network Monitor Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. AirOS contains an SNMP agent, which allows it to communicate to SNMP manage applications for network provisioning.

SNMP Agent provides an interface for device monitoring using the Simple Network Management Protocol (an application layer protocol that facilitates the exchange of management information between network devices). SNMP Agent allows network administrators to monitor network performance, find and solve network problems. For the purpose of equipment identification, it is always a good idea to configure SNMP agents with contact and location information:

SNMP Agent

Enable SNMP Agent: control will enable SNMP Agent.

SNMP Community: specify SNMP community string. It is required to authenticate access to MIB objects and functions as embedded password. The device supports a Read-only community string that gives read access to authorized management stations to all the objects in the MIB except the community strings, but does not allow write access. AirOS supports SNMP v1. The default SNMP Community is *"public"*.

Contact: specify the identity or the contact who should be contacted in case a emergency situation arise.

Location: specify the physical location of the device.

Web Server

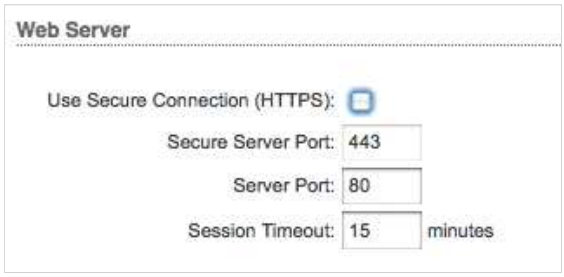
Web Server: the following AirOS v5.3 Device Web Server parameters can be set there:

Use Secure Connection (HTTPS): If checked Web server will use secure HTTPS mode. HTTPS mode is unchecked by default.

Secure Server Port: Web Server TCP/IP port setting while using HTTPS mode.

Server Port: Web Server TCP/IP port setting while using HTTP mode.

Session timeout: specifies the maximum timeout before the session expires. Once session expires you must login using device's credentials to do changes or see Main Page.



Web Server using HTTPS

SSH Server

SSH (http://en.wikipedia.org/wiki/Secure_Shell) Server: the following AirOS Device SSH Server parameters can be set there:

SSH Server

Enable SSH Server: This option enables SSH access to the AirOS Device.

Server Port: SSH service TCP/IP port setting.

Enable Password Authentication: when enabled, you must authenticate using Administrator credentials in order to grant SSH access to the device, otherwise an Authentication Key will be required.

Authorized Keys: To Import a Public key file working to get SSH access to the device instead of using an admin password, press the "Browse" button and select the key file, then press "Import" button. Finally press the "Save" button.

Telnet Server

Telnet Server: the following AirOS Device Telnet Server parameters can be set there:

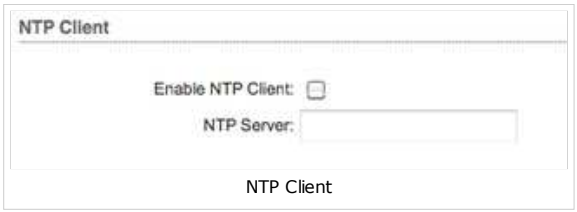
Telnet Server

Enable Telnet Server: This option activates the Telnet access to the AirOS Device.

Server Port: Telnet service TCP/IP port setting.

NTP Client

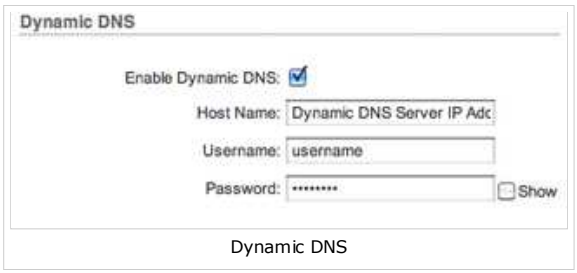
NTP Client: The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. It can be used to set the AirOS system time. *System Time* is reported next to the every *System Log* entry while registering system events if *Log* option is enabled.



NTP Client

Enable NTP Client: control will enable NTP client.
NTP Server: specify the IP address or domain name of the NTP Server.

Dynamic DNS



Dynamic DNS

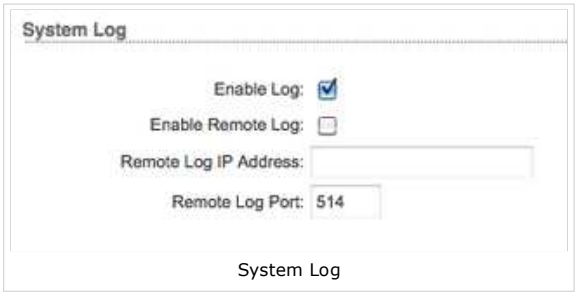
Enable Dynamic DNS: mark this checkbox to enable Dynamic DNS service for the AirOS device. Dynamic DNS is a network service providing which allows real-time notification to the DNS Server of any changes occurring in the device's IP setting, there by allowing access to the device through a Domain Name even if the device's IP address has changed.

Host Name: defines the Dynamic DNS Host Name. A large list of Dynamic DNS services is available here (http://www.dmoz.org/Computers/Internet/Protocols/DNS/DNS_Providers/Dynamic_DNS/) .

Username: defines the Dynamic DNS Username.

Password: defines the Dynamic DNS password. Check "show" to display the password.

System Log



System Log

Enable Log: This option enables the registration routine of the *system log* messages. By default it is disabled.

Enable Remote Log: enables the syslog remote sending function while *System log* messages are sent to a remote server specified by the *Remote Log IP Address* and *Remote Log Port*.

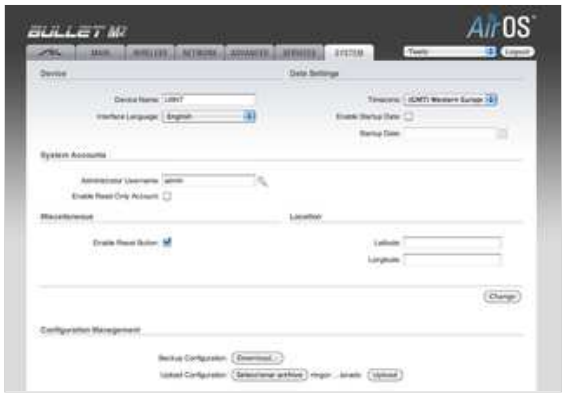
Remote Log IP Address is the host IP address where syslog messages should be sent. Remote host should be configured properly to receive syslog protocol messages.

Remote Log Port: is the TCP/IP port of the host syslog messages should be sent. "514" is the default port for the commonly used system message logging utilities.

Every logged message contains at least a *System Time* and a Host Name. Usually a particular service name which generates the system event is specifies also within the message. Messages from different services have different context and different level of the details. Usually *error*, *warning* or *informational* system services messages are reported, however more detailed *Debug* level messages can be reported also. The more detailed system messages are reported, the greater volume of log messages will be generated.

[Content]

System



System Page

The System Page contains Administrative options. This page enables administrator to reboot the device, set it to factory defaults, upload a new firmware, backup or update the configuration and configure administrator's credentials.

Device

Device Name (Host name) is the system wide device identifier. SNMP Agent reports it to authorized management stations. Device Name will be represented in popular Router Operating Systems registration screens and discovery tools.

Device Name: specifies the system identity.

Interface Language: options change the look and feel of the Web Management Interface while renaming the labels of all the configuration settings and controls according to the translation in particular language. The default language is English. The colors and the layout of all the web elements are not changed after the change of the language.

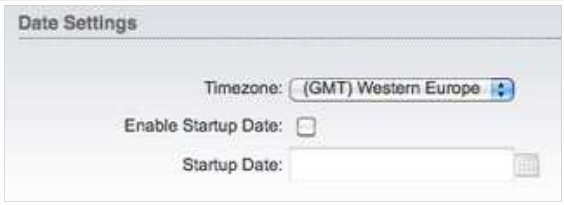
Device

Change button saves the *Device Name* if activated.

Additional language profiles may be uploaded. Please refer to this guide, which describes how to import language profile used for translation of the user interface.

Date Settings

Timezone: specifies the device's time zone according to GMT (Greenwich Mean Time). **Enable Startup Date**: when enabled, you are able to modify the device's startup date. The Startup Date is the date the devices comes back after every reboot; to maintain date and time updated configure the NTP Client feature on the Services Page. **Startup Date**: specifies the device's startup date. You may select a date by pressing the "Calendar" icon, or input it manually; type the date in the following order: 2 digits for the month, 2 digits for the day and 4 digits for the year; i.e. for the May 6th 2010 type 05/06/2010.



Date Settings

System Accounts

In this section you can modify the administrator password to protect your device from unauthorized configuration. The default administrator's password should be changed on the very first system setup:

System Accounts

Administrator Username: specifies the name of the system user.

Key button: press this button in order to change the Administrator password.

Current Password: administrator is required to enter a current password. It is required for *Password* or *Administrator Username* change routine.

Default administrator login credentials:

* User Name: ubnt
* Password: ubnt

New Password: new password used for administrator authentication should be specified.

Verify Password: new password should be re-entered to verify its accuracy.

Note: password length is 8 characters maximum, characters after the 8th position will be truncated.

Enable Read-Only Account: click to enable the read-only account, and configure the username and password to protect your device from unauthorized access. The default option is disabled.

Read-Only Username: specifies the name of the system user.

Key button: press this button in order to change the Real-only password.

New Password: new password used for read-only administrator authentication should be specified.
Show: check this checkbox in order to display the read-only password characters you have written.

Click **Change** button to save the changes.

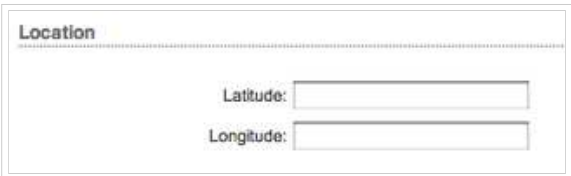
Miscellaneous

Enable Reset Button: this option allows enabling or disabling the reset button. It helps to prevent accidental device resetting to default. Although the option is disabled, the device still is able to perform a device reset through the TFTP Recovery procedure (http://www.ubnt.com/wiki/Firmware_Recovery)

Enable Reset Button

Location

Latitude and **Longitude** define the device coordinates; they are used to automatically update device location in AirControl.



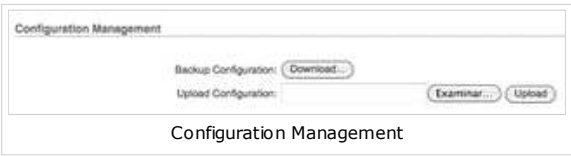
Latitude and Longitude

Configuration Management

AirOS v5.3 configuration is stored in plain text file (cfg file). Use the *Configuration Management* section controls to backup, restore or update the system configuration file:

Backup Configuration: click **Download** button to download the current system configuration file.

Upload Configuration: click **Browse** button to navigate to and select the new configuration file or specify the full path to the configuration file location.



Configuration Management

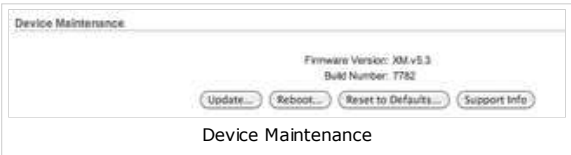
Activating the **Upload** button will transfer new configuration file to the system. The settings of the new configuration will be visible in the *Wireless*, *Network*, *Advanced*, *Services* and *System* pages of the Web Management Interface.

New configuration will be effective after the *Apply* button is activated and system reboot cycle is completed. Previous system configuration is deleted after *Apply* button is activated. It is highly recommended to backup the system configuration before uploading the new configuration.

Use only configuration backups of the same type device - configuration backed up from Bullet M2 (or M5), Rocket M2 (or M5), NanoStation M2 (or M5)! Behavior may be unpredictable when mixing configurations from different type devices. AirOS v3.4 backups are not compatible with AirOS v5.3

Device Maintenance

The controls in this section are dedicated for the device maintenance routines: rebooting, resetting, generating of the support information report.



Device Maintenance

Firmware Version: shows the current firmware version.
Build Number: displays the build number of the firmware version loaded.

Update

Use this section to update the device with the new firmware.
The device firmware update is compatible with all configuration settings. System configurations are preserved while the device is updated with a new firmware version.

Firmware section

Firmware upload

Current Firmware: displays the version of the AirOS firmware that is currently operating.
Firmware File: activate **Browse** button to navigate to and select the new firmware file. The full path to the new firmware file location can be specified there. New firmware file is transferred to the system after **Upload** button is activated.

Close this window – button cancels the new firmware upload process if activated.

Update button should be activated in order to proceed with firmware upgrade routine (new firmware image should be uploaded into the system first). Please be patient, as the firmware upgrade routine can take 3-7 minutes. AirOS v5.3 based device will be inaccessible until the firmware upgrade routine is completed.

Firmware Upload

Do not switch off, do not reboot and do not disconnect the device from the power supply during the firmware upgrade process, as these actions will damage the device!

It is highly recommended to backup the system configuration and the *Support Info* file before uploading the new configuration.

Close this window – button closes the firmware upgrade window if activated. This action will not cancel the firmware upgrade process.

Reboot: activate *Reboot* control in order to initiate full reboot cycle of the device. Reboot effect is the same as the hardware reboot, which is similar to the power off - power on cycle. The system configuration is not modified after the reboot cycle completes. Any non-applied changes will be lost.

Reset to Defaults: activate *Reset to Defaults* control in order to initiate reset the device to factory defaults routine. Reset routine initiates system *Reboot* process (similar to the power off - power on cycle). The running system configuration will be deleted and the default system configuration (all the system settings with no exception) will be set.

After the *Reset to Defaults* routine is completed, AirOS system will return to the default IP configuration (192.168.1.20/255.255.255.0) and will start operating in *Station-Bridge* mode. It is highly recommended to backup the system configuration before the *Reset to Defaults* is initiated.

Support Info: activate *Support Info* button in order to get system information file. This file should be provided to Ubiquiti support engineers (upon the request) while investigating all the technical support or configuration issues if any.

Reboot

Reset to Defaults

[Content]

Tools

Align Antenna

Align Antenna utility allows the installer to point and optimize the antenna in the direction of maximum link signal.

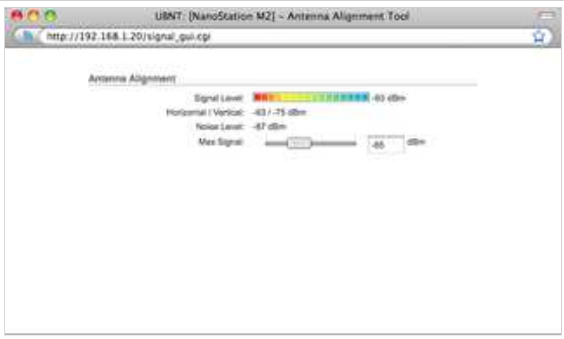
Selection of the **Align Antenna** tool will open new window with signal strength indicator. Window reloads every second displaying the signal strength of the last received packet.

Horizontal/Vertical: displays the received wireless signal levels for each polarity, while operating in Station (or Station WDS) mode on MIMO 2x2 devices. Signals Strength is measured in dBm.

"'Noise Level"': value displays the value of the noise level wireless signal was received.

The "Max Signal" slider bar allows the range of the meter to be either increased or reduced. If the range is reduced, the color change will be more sensitive to signal fluctuations as **Max Signal** slider actually changes an offset of the maximum indicator value thus the scale itself.

Align Antenna window can be closed with the **Close this window button**.



Antenna alignment Tool

Site Survey

Site Survey: utility will search for wireless networks in range on all the supported channels while device is operating in *Access Point* or *Station* mode. In *Station* mode channel list can be modified. Refer to the section *Link Setup* for the details on channel list customization.

Site Survey reports *MAC Address*, *SSID*, *Device Name*, *Encryption* type (if any), *Signal Strength/Noise, dBm*, *Frequency, GHz* and wireless *channel* of all the surrounding Access Points which can be found by the AirOs based device.

The *Site Survey* can be updated using the **Scan** button. *Site Survey* window can be closed with the **Close this window button**.

Wireless Site Survey utility

Device Discovery

This utility will scan for all Ubiquiti Network devices within the network the device is a member of. The search field will automatically filter devices containing specified names or numbers, as you type them.

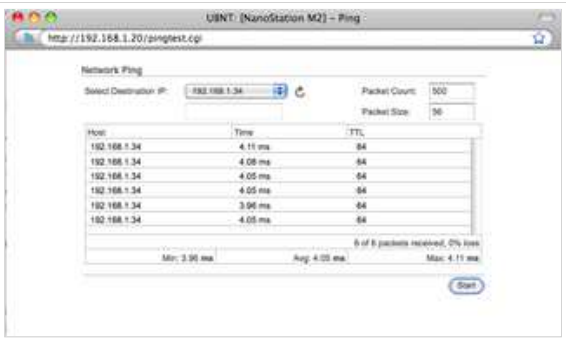
Device Discovery: shows device MAC Address, Device Name, Wireless Mode, SSID, Product type, Firmware version and IP Address. To access a device configuration through his Web GUI, click the device's IP Address.

The Discovery can be updated using the Scan button.

Device Discovery

Ping

Ping (http://en.wikipedia.org/wiki/Ping) : This utility will ping other devices on the network directly from the AirOS device.



Wireless link quality estimation with Network Ping utility

Ping utility should be used for the preliminary link quality and packet latency estimation between two network devices using the ICMP packets.

Remote system IP can be selected from the list which is generated automatically (**Select destination IP**) or can be **specified manually**.

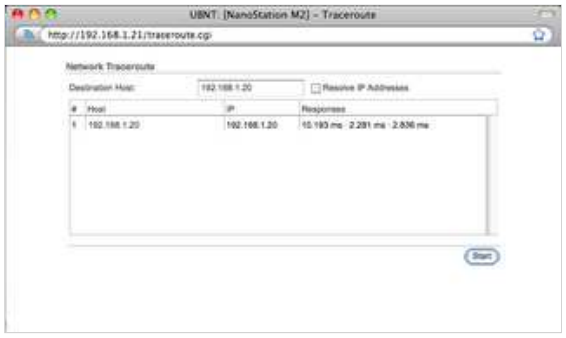
The size of the ICMP packets can be specified in the **Packet size** field. Estimation is done after the number of ICMP packets (specified in **Packet count** field) is transmitted/received.

Packet loss statistics and latency time evaluation is provided after the test is completed.

The test is started using the **Start** button.

Traceroute

TraceRoute: Allows tracing the hops from the AirOS device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the **Destination host**.



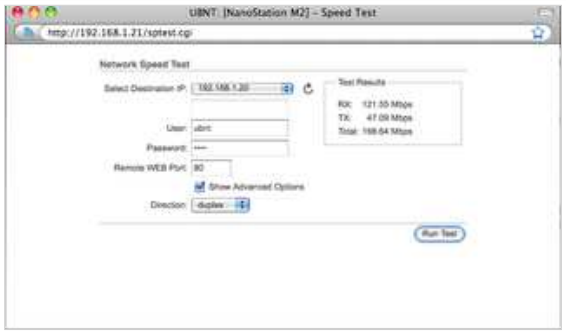
Finding the route across the network with Traceroute utility

Resolution of the IP addresses (symbolically rather than numerically) can be enabled by selecting the **Resolve IP address** option.

The test is started using the **Start** button.

Speed Test

This utility allows for testing the connection speed to and from any reachable IP address on the AirOS device network. It should be used for a preliminary throughput estimation between two network devices.



SpeedTest utility

Select Destination IP: Remote system IP can be selected from the list, which is generated automatically (Select destination IP) or may be specified manually.

Remote system access credentials (administrator username - **User** and **Password**) should be provided for the communication between two AirOS powered devices. This is required in order to establish the TCP/IP based throughput test.

Remote WEB port of the AirOS powered devices should be specified in order to establish TCP/IP based throughput test (i.e. 443 port should be specified if HTTPS is enabled in the remote system). ICMP throughput measurement routine will be initiated if the WEB port of the remote system is incorrect.

Show advanced options control will enable additional Speed Test utility options. There are 3 options available for the traffic direction while estimating the throughput maximum:

Direction:

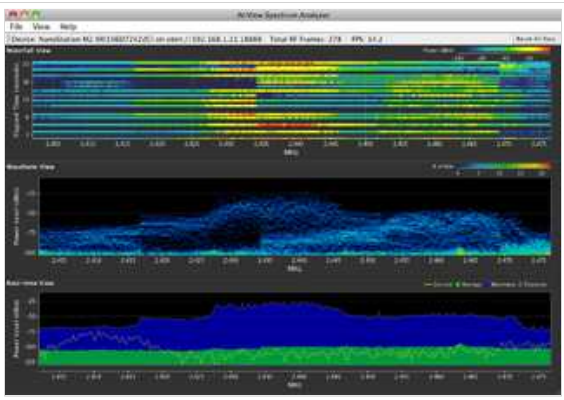
- Estimate the incoming (Rx) throughput while selecting “receive” option;
- Estimate the outgoing (Tx) throughput while selecting “transmit” option;
- Estimate the incoming (Rx) and the outgoing (Tx) throughput at the same time while selecting option duplex.

Test Results

Rx: shows the estimated incoming throughput.
Tx: shows the estimated out-coming throughput.
Total: shows the aggregated throughput

AirView

AirView is a Spectrum Analyzer included in AirOS V5.3, allowing you to see the crowdedness of the radio spectrum. A detailed step-to-step guide explaining how to use AirView is available here (http://www.ubnt.com /wiki/index.php?title=Best_channel_using_airview) .



AirView - Spectrum Analyzer

View

Enable Chart Panel 1 (top): enable this option to display the top chart, Waterfall or Channel Usage, depending on which you have selected in Preferences. These are time-based graphs showing the aggregate energy collected or Channel Usage over time for each frequency for as long as AirView has been running.

Enable Chart Panel 2 (middle): enable this option to display the middle chart, Waveform. This a time-based graph showing the aggregate energy collected for each frequency over time. The color of the energy designates its amplitude: colder colors stand for lower energy levels (with blue representing the lowest levels) at that frequency bin, whereas warmer colors (like yellow, orange or red) mean higher energy levels at that frequency bin.

Enable Chart Panel 3 (bottom): when enabled, this graph displays a traditional Spectrum Analyzer in which energy (in dBm) is shown in real time as a function of frequency. For detailed information read bellow.

Clear All Markers: Press this button to reset all the previously assigned markers. Markers are assigned by clicking a point, which corresponds a frequency, on the third chart.

Main View

Device: shows the device name, MAC and IP Address of the device running AirView.

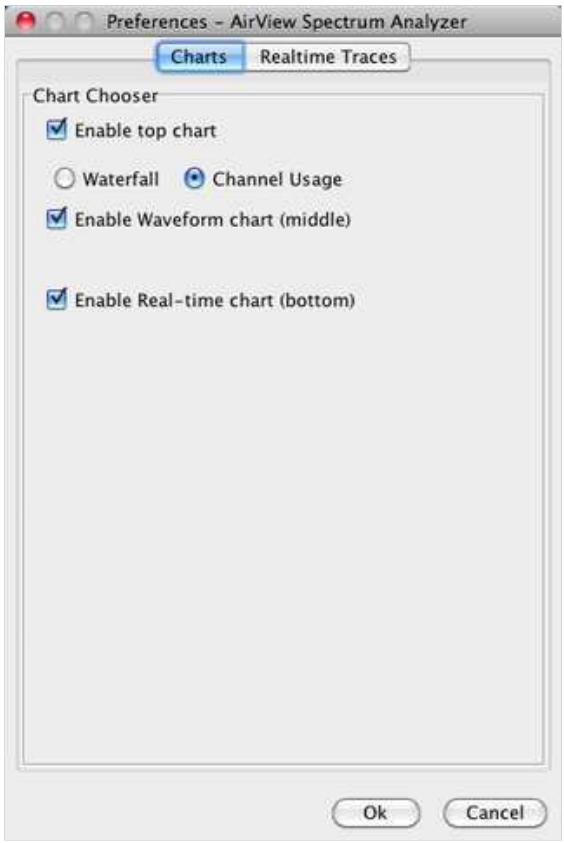
Total RF Frames: displays the total number of RF frames gathered for as long as AirView has been running or since the "Reset All Data" button was pressed.

FPS: indicates the total number of frames gathered per second. The wider the interval amplitude, the fewer frames per second will be gathered.

Reset All Data: press this button to reset all gathered data. Use this function when you want to analyze the spectrum for another place or address.

Preferences

In this section you can modify AirView Settings, such as to enable or disable charts, or specify the frequency interval.



AirView - Charts Preferences

Charts

Enable top chart: Select the chart to be displayed in the top chart on the main view. There are two options: Waterfall or Channel Usage.

Waterfall: This is a time-based graph showing the aggregate energy collected over time for each frequency while AirView has been running. The color of energy designates its amplitude: colder colors stand for lower energy levels (with blue representing the lowest levels) at that frequency bin, whereas warmer colors (like yellow, orange or red) mean higher energy levels at that frequency bin.

The Waterfall View's legend (top-right corner) provides a numerical guide associating the various colors to power levels (dBm). The low end of that legend (left) is always adjusted to the calculated noise floor, and the high end (right) is set to the highest detected power level since the start of the session.

Channel Usage: In this graph, each 2.4GHz (or 5GHz for M5-serie devices) Wi-Fi channel is represented by a bar displaying a percentage showing the relative "crowdedness" of that specific channel. This percentage is calculated by analyzing both the popularity and the strength of RF energy in that channel since the start of an AirView session.

Enable Waveform chart (middle): Like the Waterfall chart, this a time-based graph showing the aggregate energy collected for each frequency over time while AirView has been running. The color of the energy designates its amplitude: colder colors stand for lower energy levels (with blue representing the lowest levels) at that frequency bin, whereas warmer colors (like yellow, orange or red) mean higher energy levels at that frequency bin.

The spectral view over time will essentially display the steady-state RF energy signature of a given environment.

Enable Real-time chart (bottom): this graph displays a traditional Spectrum Analyzer in which energy (in dBm) is shown in real time as a function of frequency. There are three traces in this view: Max Hold - this trace will update and hold maximum power levels

across the frequency since the start of an AirView session. Average - shows the running average energy across frequency. Real-time - shows the real-time energy seen by the AirView device as a function of frequency.

Realtime Traces

The following settings apply to the Real-time chart:

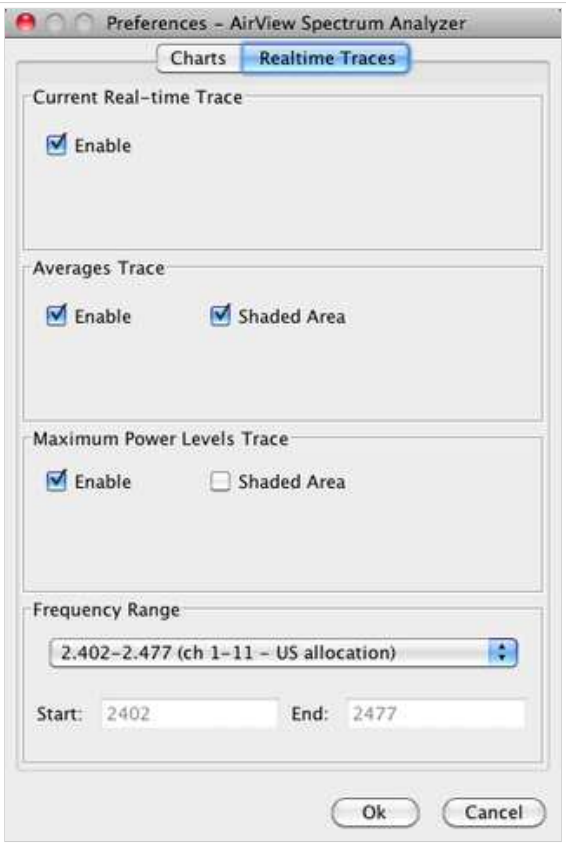
Current Real-time Trace: When the "enable" checkbox is checked the real-time trace will be turned on. This trace is the yellow outline on the chart, which represents real-time power level of each frequency. Its refresh speed depends on the FPS.

Averages Trace: This is the green area on the third chart, which represents the average received power level and considers data for as long as AirView has been running. You may disable this graph by unchecking the "Enable" checkbox. Or you may enable only a green outline, without the shaded area, by unchecking the "Shaded Area" checkbox.

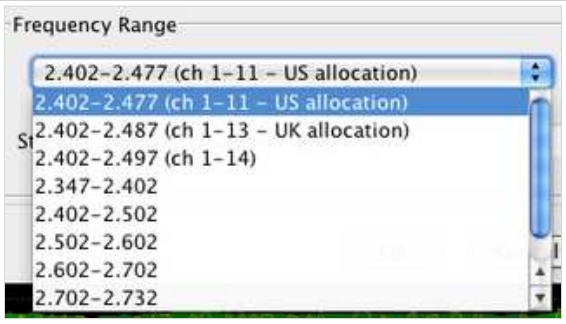
Maximum Power Trace: This is the blue area on the third chart, which represents the maximum received power level and considers data for as long as AirView has been running. You may disable this graph by unchecking the "Enable" checkbox. Or you may enable only a blue outline, without the shaded area, by unchecking the "Shaded Area" checkbox.

Frequency Range: here you can select the amplitude of the frequencies interval to be scanned. There are some pre-defined ranges for the most popular bands. However, you can specify a custom range according to your needs.

[Content]



AirView - Realtime Traces



AirView - Frequency Range